NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE USE OF INFORMATION OPERATIONS (IO) IN IMMERSIVE VIRTUAL ENVIRONMENTS (IVE)

by

Joseph V. Benson

June 2010

Thesis Advisor: Raymond Buettner
Second Reader: Steven Iatrou

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE THE USE OF INFORMATION OPERATIONS (IO) IN IMMERSIVE VIRTUAL ENVIRONMENTS (IVE)		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Joseph V. Benson			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

As the nature of warfare evolves, brute force is less applicable as an effective course of action. Constraints to conventional combat action necessitate a commander's use of less destructive means to achieve mission objectives. Information Operations (IO) employed within Immersive Virtual Environments (IVE) like *Second Life* is potentially capable of meeting that requirement. The growing popularity and pervasiveness of IVEs present new opportunities and vulnerabilities as compared with more traditional methods of IO. Interactions within IVEs have measurable social and economic impacts in the physical world. The use of IO in IVEs can bring exponentially disproportionate effects relative to the effort required. China is a prime example of a potential antagonist that is likely to exploit IO in IVEs. China's modern warfare strategies are built around asymmetry. This includes the justification of pre-emptive offensive cyber attacks. It is reasonable to expect China and others to expand their cyber warfare portfolio to include the use of IO in IVEs. The United States cannot afford to ignore this real and emerging threat. Continued research into developing this capability provides assurance that DoD will realize the potential in this area before falling victim to adversarial exploitation of the same.

14. SUBJECT TERMS Immersive Virtual Environment, IVE, Information Operations, IO, Influence, Virtual World, China, Information Warfare, Avatar, Transformed Social Interaction, TSI, Captology, Massively Multi-player Online Roll-Playing Game, MMORPG, Cyberspace, Cyber-Warfare.			**15. NUMBER OF PAGES** 87
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE USE OF INFORMATION OPERATIONS (IO) IN IMMERSIVE VIRTUAL ENVIRONMENTS (IVE)

Joseph V. Benson
Captain, United States Marine Corps
B.S., Old Dominion University, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
June 2010

Author: Joseph V. Benson

Approved by: Raymond Buettner
Thesis Advisor

Steven Iatrou
Second Reader

Dan C. Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As the nature of warfare evolves, brute force is less applicable as an effective course of action. Constraints to conventional combat action necessitate a commander's use of less destructive means to achieve mission objectives. Information Operations (IO) employed within Immersive Virtual Environments (IVE) like *Second Life* is potentially capable of meeting that requirement.

The growing popularity and pervasiveness of IVEs present new opportunities and vulnerabilities as compared with more traditional methods of IO. Interactions within IVEs have measurable social and economic impacts in the physical world. The use of IO in IVEs can bring exponentially disproportionate effects relative to the effort required.

China is a prime example of a potential antagonist that is likely to exploit IO in IVEs. China's modern warfare strategies are built around asymmetry. This includes the justification of pre-emptive offensive cyber attacks. It is reasonable to expect China and others to expand their cyber warfare portfolio to include the use of IO in IVEs.

The United States cannot afford to ignore this real and emerging threat. Continued research into developing this capability provides assurance that DoD will realize the potential in this area before falling victim to adversarial exploitation of the same.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CNA	Computer Network Attack
CNO	Chief of Naval Operations
CNO	Computer Network Operations
CVE	Collaborative Virtual Environment
DoD	Department of Defense
DOS	Denial of Service
EW	Electronic Warfare
FITE	Future Immersive Training Environment
HCI	Human-Computer Interface
IO	Information Operations
IVE	Immersive Virtual Environments
IVEA	Intelligent Virtual Environment Agent
IW	Information Warfare
JP	Joint Publication
MILDEC	Military Deception
MMORPG	Massively Multi-Player Online Role-Playing Game
NZSMG	Non-Zero Sum Mutual Gaze
OPSEC	Operational Security
PLA	People's Liberation Army
PSYOP	Psychological Operations
RFP	Request for Proposal
SSG	Strategic Studies Group
TA	Target Audience
TSI	Transformed Social-Interaction
TTP	Tactics, Techniques, and Procedures
VE	Virtual Environment
VHIL	Virtual-Human Interaction Lab
VoIP	Voice Over IP

VR	Virtual Reality
VTC	Video Tele-Conference
VW	Virtual World

EXECUTIVE SUMMARY

The ability to influence the thoughts and behaviors of people is an important tool. Influence provides commanders the means to shape the physical, informational, and social environment. In the military, this is accomplished through the use of Information Operations (IO). IO has become an integral part of the successful execution of most military operations. The tools available through IO provide a commander the ability to influence people, environments, and information. This is as true in virtual environments as it is in the physical world.

Virtual environments are easily conceptualized as computer-simulated environments that simulate places in the real world. Immersive Virtual Environments (IVE) take this concept a step further by perceptually surrounding the user. They provide a sense of being enveloped by, included in, and interacting within the environment. Users can directly interact with other users through manipulation of their avatars—digital representations of themselves.

IVEs, such as *Second Life*, are growing in popularity. The growing popularity and pervasiveness of these environments is translating into a growing user base of individuals and groups spanning the globe. IVEs like *Second Life* are powerful environments that generate real human responses through real human interaction. The impact of interaction in these environments transcends the virtual environment and has measurable social and economic impact in the physical world. Because of this, IVEs present unique and evolving opportunities for the use of IO by its users. The employment of IO in IVEs by adversaries of the United States is a risk that must be addressed.

China is a prime example of a potential antagonist that is likely to exploit IO in IVEs. China's modern warfare strategies are built around asymmetry. The Chinese interpretation of asymmetry includes the justification of pre-emptive offensive cyber attacks to discourage adversaries. The use of cyber warfare is one of the pillars of its asymmetric mindset. There are many recent examples where China has demonstrated an

uninhibited willingness to engage in cyber attacks. It is reasonable to expect China to expand its cyber warfare portfolio to include the use of IO in IVEs.

The Chinese are highly likely to employ this type of asymmetric cyber attack but they are not the only ones that possess the potential. Implementing IO in IVEs only requires a computer and Internet access; exploitation may begin with a task as simple as creating a user account. In contrast, hacking requires more advanced skill sets and education. The exploitation of IO in IVEs has exponentially disproportionate effects relative to the effort required. This presents a threat potential that the United States must address immediately.

The United States must provide education that allows IVE users to recognize indicators of potential adversarial use of IO in these environments. Using the Marine Corps as an example, recommended implementation would center on familiarization and PME-based training. Familiarization of the use of IO in IVEs would be implemented during initial and annual refresher training. This training would be integrated with existing guidance surrounding responsible use of Internet-based capabilities similar to that outlined in MARADMIN 181/10. PME-based training would be integrated into existing SNCO and Officer PME curriculums providing a more in-depth look at the operational potential of IO in IVEs, to include its effects in support of both offensive and defensive operations.

The United States cannot afford to ignore this real and emerging threat. Training that is developed should be tailored to the roles of enlisted and officers. OPSEC awareness must be stressed at all levels. U.S. military operations and dominance in the land, sea, and air domains are dependent on maneuver and dominance in the cyberspace domain. Cyberspace operations must include development of Tactics, Techniques, and Procedures (TTP) for offensive and defensive employment of IO in IVEs and similar virtual environments. Continued research into developing this capability provides assurance that DoD will realize the potential in this area before falling victim to adversarial exploitation of the same.

ACKNOWLEDGMENTS

I owe sincere appreciation to Joel Scharlat for introducing me to the possibilities that exist within virtual environments. Thank you for taking the time to discuss your thesis work with me and suggesting related research opportunities. Your input and recommendations laid the foundation for my research.

I would like to express my sincere thanks to Ray Buettner, Steven Iatrou, and CDR Michael Herrera for all of your guidance and assistance in the completion of my thesis. Your unwavering patience and support were instrumental in its successful completion.

To Dave Ferrasci and Nelson French, words alone are insufficient to express my gratitude for everything you have done to contribute to this work. Your material support and assistance were critical to completing this work, but I am most appreciative for your friendship.

Finally, to my wife, Pam, my mother, Mary Jane, my father, Barry, and all of my family, this accomplishment is as much yours as it is my own. Your love, tireless support, and understanding through this journey ensured I never lost sight of the final objective, and are in large part responsible for my success.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The ability to influence the thoughts and behaviors of people, whether adversaries, partners, civilians, or military, is an important tool. Influence provides commanders the means to shape the physical, informational, and social environment around him. This is accomplished through use of Information Operations (IO). IO has become an integral part of the successful execution of most military operations. The tools available through IO provide a commander access to people, places, and information.

This is as true in virtual environments as it is in the physical world. Immersive Virtual Environments (IVE) such as *Second Life*[1] are growing in popularity. The growing popularity and pervasiveness of these environments is translating into a growing user base of individuals and groups spanning the globe. The ability to influence the thoughts and behaviors of people, combined with the growing popularity and pervasiveness of IVEs like *Second Life*, present new opportunities and vulnerabilities as compared with more traditional methods of IO.

The term Information Operations (IO) is a recent development; however, the underlying concepts are nearly as old as warfare itself. As early as the 12th century BC, when the Greeks used the Trojan horse to gain entrance to the city of Troy, IO has been an integral part of warfare [1]. Joint Publication 3–13 [2], published by the U.S. military in 1998 and updated in February 2006, defines IO as, "The integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial decision making while protecting our own." The publication further categorizes the core, supporting, and related capabilities by their objectives and intended targets/audiences. JP 3–13 serves as the definitive guide for the conduct of IO within the

[1] An Immersive Virtual Environment created and maintained by its users.

Department of Defense (DoD). It explains in detail what IO is and its relative importance to military operations.

JP 3–13 defines and aggregates the information environment into three relevant dimensions: physical, cognitive, and informational. The physical dimension is composed primarily of command and control systems and supporting infrastructures. The informational dimension is where information is collected, processed, stored, disseminated, displayed, and protected. The cognitive dimension is described as the area where human decision making takes place, and the location of such intangibles as morale, unit cohesion, public opinion, situational awareness, perceptions, emotions, and understanding. This thesis and the concepts and theories discussed are focused on the exploitation and influence of the cognitive dimension through the use of IVEs.

B. RESEARCH QUESTION

This thesis will examine IVEs and their applicability in the conduct of IO. It will examine IVEs and establish a common understanding of their context and importance in cyberspace and the daily lives of humans. This thesis will address the following research question:

Is it possible to effectively leverage Information Operations in an Immersive Virtual Environment?

C. SCOPE

This thesis builds upon our existing understanding of cognitive science as it relates to influencing human behavior. Specifically, this thesis evaluates a theory surrounding the efficacy of the use of Information Operations within Immersive Virtual Environments. In recent years, interest surrounding this potential capability has grown resulting in the increased availability of related research studies. For example, Joel Scharlat's master's thesis explored the application of autonomous agents as IO tools in virtual environments [3]. Direct interaction with Joel Scharlat served as partial inspiration for creation of this thesis.

Scharlat's work explored the general use of autonomous agents in the virtual world. The work focused primarily on the creation and implementation of an Intelligent

Virtual Environment Agent (IVEA) as it applies to a specific target set in the virtual world. This agent would operate autonomously or semi-autonomously within IVEs, primarily as an intelligence gathering tool [3].

While both theses share an overview of IVEs, this thesis explores the broader and more universally applicable concept of leveraging IO in an Immersive Virtual Environment independent of any specific implementation method, and free from the constraints of existing IO doctrine. By carefully examining these environments in this context, conclusions can be drawn regarding the potential effectiveness of employing IO capabilities within them.

D. METHODOLOGY

This thesis will introduce IVEs as they relate to Information Operations. Analysis will be conducted to determine the applicability and potential effectiveness of IO capabilities within IVEs. China will be used as an exemplar antagonist to illustrate adversarial opportunities and advantages and our own vulnerabilities and limitations to the employment of IO in IVEs. The conclusions and recommendations presented in this thesis are intended to motivate the DoD to further study this emerging battlespace.

E. THESIS ORGANIZATION

Chapter I: This chapter describes the IVE battlespace and its potential for military and intelligence exploitation. It also describes the format of the thesis.

Chapter II: This chapter provides an introduction to IVEs, a detailed introduction to *Second Life*, and a literature review of relevant research.

Chapter III: The operational relevance of IVEs is established by mapping IVEs to IO.

Chapter IV: Using China as an exemplar, a case-study evaluation is made that reveals potential threats and vulnerabilities relative to IO in IVEs.

Chapter V: This chapter concludes the thesis with an overview of the conclusions reached and offers a list of follow-on research questions and topics.

THIS PAGE INTENTIONALLY LEFT BLANK

II. IMMERSIVE VIRTUAL ENVIRONMENTS

A. INTRODUCTION

In order to effectively articulate the potential value of IO in IVEs, a common baseline understanding of the environments and the associated sciences must be established. This Chapter provides that baseline understanding through a general introduction to IVEs, a detailed introduction to *Second Life*, and a literature review of relevant studies surrounding human behavior and the interaction of computers and humans.

B. VIRTUAL ENVIRONMENTS

As the growth and popularity trends of IVEs and similar online games continue to rise, it becomes more important to provide accurate terminology to the medium. Virtual Reality (VR), Virtual Environment (VE), Virtual World (VW), Immersive Virtual Environment (IVE), and Massively Multi-Player Online Role-Playing Game (MMORPG) are terms often used interchangeably by the media. These worlds or environments possess similar characteristics; however, they are not intuitively discernible without a more precise definition of these terms.

Virtual Reality is a technology that allows the user to interact with a computer-simulated environment. This term has been both widely used and often exaggerated creatively by movie producers and science-fiction writers for years. As a result, both misconceptions and inflated expectations exist surrounding it. In general, VR is assumed to be a blanket descriptor for a wide array of applications involving immersive, 3-Dimensional (3-D), highly visual environments. Thus, all of these items could be said to be forms of VR.

In this thesis, virtual environments are defined as "synthetic sensory information that leads to perceptions of environments and their contents as if they were not synthetic" [4]. Virtual *world* and virtual *environment* can be viewed as synonymous. While VEs can offer a sense of interaction between the user and the environment, this is not a specific requirement. Digital computers are typically used to create images within these

environments and enable real-time interaction between the users and the VE. Users can interact with a VE using any perceptible channel, including visual, auditory, olfactory, gustatory, or haptic (e.g., by wearing gloves that offer mechanical feedback or through the use of air blasts directed toward the hands when a person makes contact with an object in the VE). Any combination of these can be used to create effective interaction. Consider a common home computing environment wherein a user interacts with a VE through a computer. His computer has a monitor (visual channel) and speakers (auditory channel).

An IVE takes the concept of a virtual environment one step further. An IVE is an environment that perceptually surrounds the user of the system [4]. An IVE provides a sense of being enveloped by, included in, and interacting within the environment. The sensory information of an IVE is more psychologically prominent than the sensory information of the real world. This is accomplished through the employment of three characteristic features.

First, the user takes on the actual point of view of a character or avatar[2] within the environment. Figure 1 depicts example avatars that exist in *Second Life*. Through some form of input,[3] the user is able to control the avatar's movement and interactions within the environment. Second, sensory information from the physical world is kept to a minimum. For example, headphones or earphones could provide auditory isolation by blocking out ambient noise. Finally, an IVE would typically provide realistic look and feel by creating virtual representations of physical locations.

[2] An avatar is a 2- or 3-dimensional digital representation of the user [5].

[3] Keyboard and mouse commands could be used for movement and point of view. A microphone and speakers could be used for speech interaction with the IVE.

Figure 1. Avatars in *Second Life*. From [4]

One example of an IVE in use today is a product from Linden Research, (commonly referred to as Linden Labs) known as *Second Life*.[4] Released to the public in June 2003, *Second Life* is a 3-D virtual world that is patterned after the physical world. *Second Life* allows users (referred to as "Residents"[5]) to freely interact with one another through their avatars. Resident avatars have the ability to socialize, participate in group activities, obtain employment, create and trade virtual property, and exchange or use services with each other [5].

Massively Multi-Player Online Role-Playing Games are very similar to IVEs. In fact, examination of most MMORPGs reveals that they satisfy the definition of an IVE. Similarities notwithstanding, there is a large intersection between MMORPGs and IVEs. *World of Warcraft* [7] is one of the more popular MMORPGs in use today. User interaction and capabilities within *World of Warcraft* are very similar to those found in *Second Life*. Still, two key differences provide a clear distinction between them.

[4] *Second Life* will be referenced throughout this thesis as an exemplar IVE for illustrative purposes.

[5] A "Resident" is a uniquely named avatar within *Second Life*.

MMORPGs users are goal oriented. These worlds generally offer quests or missions for their users that offer rewards for successful completion. Users in these worlds acquire wealth and stature through the completion of tasks and objectives. *Second Life* is independent of any goal or objective. *Second Life* is simply a place for users to interact freely.

The MMORPG environment is finite, constrained by a fixed size. For example, in *World of Warcraft*, the environment is comprised of two continents on the world of Azeroth [8]. In contrast, the *Second Life* environment is infinite. Users create land space within the world. The world can grow as large as the users make it. *Second Life* is organized into a mainland region with satellite private regions or islands surrounding. The mainland region is a group of connected regions where users can own, lease, or buy existing space. The private regions or islands are not connected to the mainland. Instead, they are placed around the mainland. These represent the growth potential for the world. These regions can be coupled together to form mini continents or used individually. There is no limit to the number of private regions that can be added to *Second Life* [9].

IVEs, with their growing popularity and proliferation into our everyday lives, represent a new and seemingly unexplored area for the conduct of military operations.

C. UNDERLYING ASSUMPTIONS

1. Cyberspace

Joint Publication 1–02 [10] defines "cyberspace" as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." The DoD definition is easy to grasp or understand because it describes a physical instantiation; the current platform for operations in cyberspace. It gives cyberspace physical characteristics that can be internalized and assessed finitely.

A Chief of Naval Operations (CNO) Strategic Studies Group (SSG) concept paper written by Will Koszarek in 2007 [11] discusses the limitations of this definition. Koszarek explains how we are unable to recognize the full exploitation potential when

defining an operational domain in terms of its physical characteristics or the "what" [11]. He suggests that Cyberspace must be viewed outside the constraints of the physical infrastructure or specific technology upon which it exists.

> If we think of cyberspace as a medium for operations like the air or sea domains then limiting our understanding of cyberspace to "a domain characterized by the use of electronics and the electromagnetic spectrum….." is similar to describing the maritime domain as a medium characterized by ships and shipping routes to exchange goods or the air domain as characterized by the presence of various airframes to transport people. All of these statements are factual but they also serve to limit our understanding of the domain being considered. Consequently if we devise our operations and capabilities solely on these understandings then we will greatly limit what is possible and increase our vulnerabilities. [11]

This thesis replaces the DoD definition with the alternate as described by Scharlat [3]. Referring to the CNO SSG concept paper [11], Scharlat described Cyberspace as a collection of links. That characterization serves to effectively decouple our understanding of what cyberspace is from what particular technology supports it. All the links provide, intentionally or otherwise, a connection of individuals around the world [11]. The presence, growth, and persistence of these links provide unprecedented potential for influence.

2. Real Access

Look around you at any time and you will see an extensive proliferation of electronic network devices. BlackBerries and similar handheld devices connect users to the Internet and provide chat, email connectivity, as well as Voice over IP (VoIP). Cellular phones allow global voice connectivity independent of physical infrastructure (e.g., building or vehicle). Laptop computers and wireless access technology allow us to "reach" cyberspace from just about anywhere. The Internet and these technologies have created the ability to connect with anyone in the world instantly. IVEs represent the latest evolution of human-human interaction through technology.

3. Key Metrics

Examination of key metrics of our exemplar IVE *Second Life* provide some perspective regarding the growing popularity of these worlds, as well as the level of real access these worlds provide to their users. Figure 2 shows *Second Life* population data as of May 23, 2010. Currently, over 19 million Residents occupy *Second Life*. Put in perspective, only three states in the U.S. have larger populations: New York, Texas, and California [12].

Reflects data through midnight, 23 May

Population

Residents Logged-In During Last 7 Days	581,623
Residents Logged-In During Last 14 Days	750,599
Residents Logged-In During Last 30 Days	1,017,295
Residents Logged-In During Last 60 Days	1,421,779
Total Residents	19,313,467

Figure 2. *Second Life* Population Data, May 2010. From [12]

Figure 3 depicts a significant increase in the number of Resident user hours from 2006 to the end of the first quarter of 2008. From 4th quarter 2007 to 1st quarter 2008 alone, Resident user hours grew 15% from an annualized rate of 304 million hours to just under 350 million user hours. To put those numbers in perspective, if the 350 million user hours are distributed equally among the 19 million total Residents in Figure 2, each user would be using *Second Life* for 36 minutes every day for the entire month.[6]

[6] (350 million hrs/month) / (19,313,467 users) = (18.12 hrs/person/month) →(18.12 hrs/person/month) / (30 days/month) = (.604 hrs/day) == 36 minutes per day average usage.

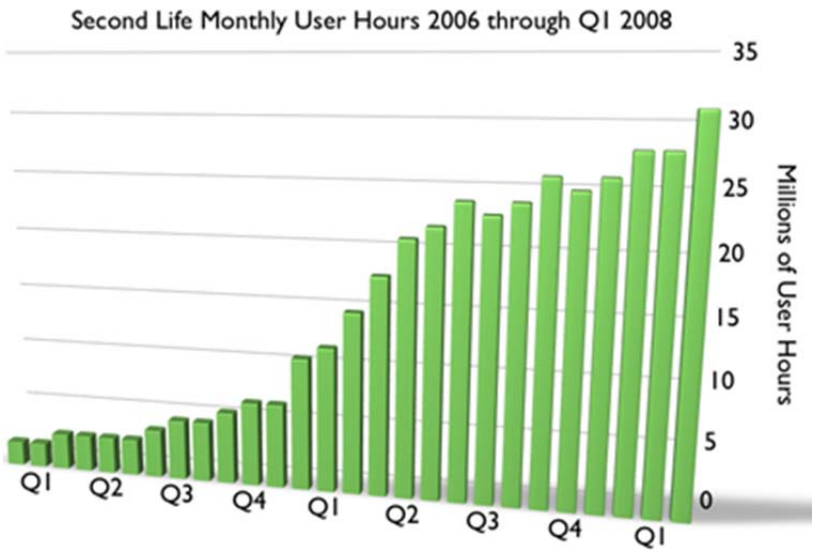

Figure 3. *Second Life* Monthly User Hours. From [13]

Figure 4 depicts the number of unique users with repeat logins from the first quarter of 2008 through the end of the first quarter of 2010. The number of repeat users grew 33% over the period from 555,000 to 826,000 between first quarter 2008 and first quarter 2010.

Figure 4. *Second Life* Unique Users with Repeat Logins. From [14]

4. Real Economies

The *Second Life* environment has a fully-integrated economy with its own form of currency. The Linden dollar, or L$, is a form of currency that Residents can use to pay for goods and services within *Second Life* [16]. Linden dollars can be purchased and sold through the Linden Exchange (LindenX) for real U.S. dollars or other currency. Linden dollars or U.S. dollars can be used within *Second Life* for the completion of financial transactions.

In *Second Life*, users are allowed to create content within the environment (e.g., avatar clothing). There is no cost associated with creating content and the creators retain legal rights to that content. They can sell created items in the world to other Residents in exchange for Linden dollars or U.S. dollars [17]. Thousands of Residents make part or all of their real-world income from their *Second Life* businesses [17].

In addition to created content, Residents of *Second Life* can buy and sell land and charge fees for use of services on their land. For example, a Resident might own land on which he built a night club. He may charge an entrance fee to enter the club. Users may also seek employment and receive compensation within *Second Life*. In the aforementioned night club example, the Resident who owns the night club may hire other Resident avatars to provide services within the club such as DJ, bartender, bouncer, and other services associated with club operations in the physical world.

Figure 5 shows the annual values in millions of U.S. dollars relating to user transactions within *Second Life* between 2007 and 2009. An average of $414.67 million has been exchanged between users of *Second Life* every year since 2007. The economic data for *Second Life* alone gives perspective and scale to the potential economic impact all IVEs possess in the physical world.

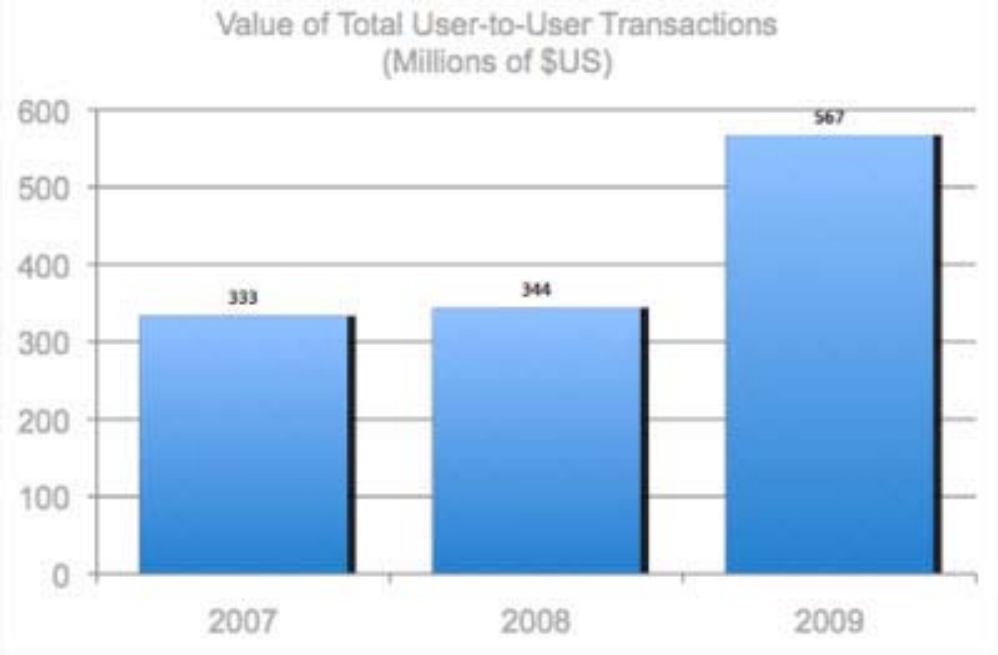

Figure 5. *Second Life* User-to-User Transaction Values. From [17]

D. THE SOCIAL INTERACTION OF COMPUTERS AND HUMANS

1. Introduction

The previous section demonstrates the impact of IVEs among a large and growing segment of the human population. The amount of interaction between humans in these worlds suggests there is an increased potential to reach larger numbers of people. That potential provides opportunities to affect influence. In order to take advantage of those opportunities, the social interactions of humans must be explored.

2. The Small World Effect

While interest in how connective technologies such as IVEs are affecting our social interactions is somewhat new, the idea that one person can be connected to another through a series of links is not. The theory commonly known as “six degrees of separation” was first published in a paper written by Stanley Milgram in 1967. His theory describes the “small world” effect. His study concluded that people in the U.S. could be connected to any other person in the U.S. by an average of 5.5 links [19].

The growth and increasing use of connective technologies like IVEs have changed the landscape. Findings from a more recent study comparable to Milgram's were published in 2003. The findings suggest that the average link between any two people on the planet has shrunk to approximately 4 degrees [20]. On its face, the reduction in connections by roughly 2 degrees is perhaps neither surprising nor particularly noteworthy to most. However, pointing out a couple key differences in the experiments serves to illustrate the huge significance of this change.

Stanley Milgram's experiment was conducted using paper-based messages that had to be physically transferred between people. His experiment was carried out within the United States. In contrast, the 2003 study was conducted globally spanning 13 countries. Messages in the latter experiment were transferrable via Email. As evidenced by the findings in 2003, individual extended networks are exponentially larger. This appears to be a direct result of connective technology expanding and evolving to provide greater access to individuals.

3. The Human Element

In Chapter I, IO capabilities and the information environment were introduced. JP 3–13 defines the information environment as the combination of "…individuals, organizations, and systems that collect, process, disseminate, or act on information" [2]. Of those three elements, individuals represent the greatest threat to the security of information.

Information within organizations can be protected through physical security measures. Consider military installations with layered physical security controls. These controls at the outer most layer limit access to the installation itself. Within the installation, additional layers of security provide greater scrutiny to limit physical access to information. Systems are comparably secured. IT computer systems are secured by network administrators who apply physical and electronic safeguards against network attack. In addition to physical controls, sensors or alarms can be used to provide warning or notification of attempts to gain unauthorized access to information.

Information possessed by individuals cannot be comparably protected through physical security measures. Training and education are the primary tools used. The military and many companies in industry have been providing standardized training to their members for years on the hazards and risks of disclosure of sensitive information. Related training is provided that teaches members to recognize intelligence collection techniques in an effort to safeguard this sensitive information.

In spite of these efforts, exploitation of the human element of the information environment still occurs with relative ease. Seemingly unsophisticated social engineering attacks are often successful. Consider two examples, phishing and pretexting.

A phishing scam is one method used to circumvent safeguards and obtain private or organizational information. A phisher[7] makes a seemingly legitimate request for you to reveal some personal information. These scams are particularly effective because they present a plausible set of circumstances. For example, an individual or group may create an email that appears to originate from your banking institution. The email alerts you of fraudulent account activity and requests you verify your account information through a web link provided in the message in order to continue to use your account. Your personal information is captured when you provide it on the fraudulent website. A phishing scam adapted to *Second Life* might be where an avatar provides you with a link to a malicious website and promise compensation in Linden dollars for simply signing in using your *Second Life* username and password.

Another equally effective method is pretexting. Pretexting involves creating and using an invented scenario intended to persuade a target to release specific information. Typically done over the telephone, this scam uses pieces of information about a target victim (e.g., name, address, telephone number) to establish legitimacy and gain the trust of the victim. Once trust is established, it is fairly easy to get the victim to reveal more personal information. This technique can also be used to obtain customer information from a business in the same manner. This scam is easily adapted to an IVE. For example,

[7] In the context of computer security, a phisher is a tech-savvy con artist. He or she uses fake websites, spam, e-mail, instant messaging, or other techniques that ultimately lead to an unsuspecting individual to reveal sensitive personal information such as usernames, passwords, (bank) account data, or other personal identifying information.

an avatar might give you an object or gift that requires you to reveal your Second Life password before it can be opened. In fact, *Second Life* does not require password authentication for anything in world after initial login [21].

As mentioned, training is routinely conducted that attempts to safeguard against these social engineering threats. However, this training is incomplete because of an assumption that it applies only in the physical world and workplace. This unintentional bias overlooks applicability to IVEs and exposes DoD service members to risk and potential exploitation.

A service member will find obvious relevance and context in the physical world when told not to disclose sensitive information about himself or his military assignment. However, he may not automatically assume comparable relevance to disclosure of that same information in an IVE. A hypothetical but plausible scenario is used to illustrate the point.

Specialist Snuffy is stationed overseas at a sensitive communications installation. His work week concluded with his attendance of annual required training for Information Assurance and OPSEC. When he arrives home, he logs into his *Second Life* account and begins to relax at some of his favorite virtual hangouts, starting with his favorite virtual club. A short time after he arrives, he is approached by a young female who strikes up a conversation and sits down. They make small talk for a while and the conversation moves to exchanges about where they each work. The woman ambiguously explains she works for a human resource firm that looks for active and former military members of the United States who possess unique knowledge and skills that might benefit her organization. She then redirects the conversation quickly back to talking about Specialist Snuffy and seems very impressed and interested in the details of his job. The attractiveness of this woman and her apparent interest in Specialist Snuffy helped him to let his otherwise vigilant guard down. He feels more relaxed and comfortable without having to worry about the possibility that he is a target of intelligence gathering or IO.

The longer they talk and the more comfortable he becomes, the more interested the woman appears. As time passes, the conversation begins to focus on more specific details of his job to include details of security at the facility, etc. He tells a story he considers funny about a particular gate guard who is chronically found asleep on post. Specialist Snuffy finishes the story, providing details of the guard's name and fixed rotation schedule. They both exchange a laugh and his gaze rises as he tips his glass up to finish his drink. When his gaze returns to the woman, he catches the last glimpse of her as her avatar disappears from his monitor.

This is a plausible set of circumstances to those in the IVE community. Any service member in any environment can be the target of intelligence gathering or IO. Current Information Assurance and OPSEC training do a good job of preparing our service members to recognize possible threats like the one described above when it occurs in the physical world.

Cyber-related threats are presumed to occur and anticipated through phishing scams, hacking, or similar attacks. Those attacks are executed online. Specialist Snuffy failed to recognize his risk exposure within the IVE because he did not associate the IVE as part of the online threat environment.

Specialist Snuffy's naiveté can be partially explained by the perception of anonymity inherent with human interaction on the Internet. In physical interactions, it is difficult to change or mask your identity. Once engaged, it can be difficult to quickly remove yourself from a physical interaction, particularly if that interaction becomes uncomfortable or hostile. In online interactions, there is no direct physical contact so identities can be protected. Users can log off at any time and remove themselves from compromising situations. This leads to a sense of anonymity and control.

The perception of anonymity is stronger in IVEs because of the ability to alter the characteristics of the avatar, allowing the user to obfuscate any perceptible identification of them. Manipulating characteristics of the avatar reinforces a feeling of safety which leads to a false sense of security which translates to decreased vigilance. Users in IVEs will subsequently exercise less caution and be less aware of threats around them. Since

this is a human characteristic, we can exploit it in an offensive role (adversaries are equally at risk). However, we are equally susceptible and must therefore defend against it.

Consider an adversary who configures avatars as non-threatening representations of everyday people. That adversary would have limited success winning your trust if he were to create an avatar that appeared as a suicide bomber or enemy combatant. But an adversary presented as an attractive innocuous woman like the one who approached Specialist Snuffy, or one that appears to be a fellow U.S. soldier, perhaps wearing a U.S. Army T-shirt that Snuffy would find familiar, might be much more successful. Through manipulation of elements of Self-Representation[8] an adversary can manipulate his avatar's appearance in order to maximize his impact on the intended target.

Our training provides us some reasonable and obvious heuristics that assist with spotting attempts to solicit sensitive information or conduct IO against us in the physical world. But as mentioned, our training focuses on the workplace and logical extensions to it. We often discuss Web-based threats; however, they are usually limited to spoofed websites and email phishing attacks. There is still a mental disconnect between IO threats and online environments, and an even greater disconnect between IO and IVEs. This disconnect represents a seam between current thought of our exposure and risk in IVEs to what is actually possible. This seam is a huge vulnerability that our adversaries could exploit.

All electronic communication on the Internet shares one common characteristic. The exchanges between electronic devices communicate through bits on a wire. This includes commands sent to an avatar in *Second Life* to tell it to move and verbal communication between two users through an audio chat program. While the surface of *Second Life* offers a perception of anonymity, a determined adversary with simple

[8] Self-Representation is the strategic decoupling of the rendered appearance or behaviors of an avatar from the actual appearance or behaviors of the human driving it. This element of Virtual Human Interaction (VHI) is described by Dr. Jeremy Bailenson and co-authors in [21], which introduces the concepts of Transformed Social Interaction (TSI). It is described in greater detail in the Virtual Human Interaction section of this thesis.

software tools and education could intercept those bits in transit and trace an individual from *Second Life* back to a specific computer.

Consider two users interacting in *Second Life*. They are discussing music. User A tells user B he has free music available for download on his website. He gives User B a link to his website. User B visits the website to download the music. User A could track User B's visit in a variety of ways. Malicious code could be attached to one of the downloaded files. The website computer code could be written to capture the IP address or other identifying information. A router or firewall as part of the hardware string supporting the website could be employed to log incoming activity. Perhaps the simplest method would be through the use of a freely available software tool like Wireshark [23]. Designed to be a diagnostic and troubleshooting network tool, Wireshark can be used to capture and see all traffic passed over any network. Any of these methods could be used to capture identifying information about User B or his computer. That information, alone or coupled with social engineering efforts, could then be used to indentify User B in the physical world.

4. The Media Equation

It would be correct to refer to IVEs as pieces of software; however, this definition is grossly inadequate, as it understates IVE relevance and importance in today's information environment. IVEs represent a growing and persistent trend in cyberspace. This trend strives to provide an emotionally and intellectually vibrant experience for the user. This is accomplished by providing an immersive virtual environment that has similar look and feel to the user's physical environment.

IVEs are designed to solicit cognitive responses from humans as a result of interactions through and in the immersive environments they provide. They accomplish this through direct application of the media equation. The media equation is a theory developed by Byron Reeves and Clifford Nass in a book published in 1996 that proposes human interaction with computers, television, and other media are fundamentally the same as those that occur between humans in real life. Reeves and Nass believe that we unconsciously and automatically respond to communication media as if they were

human. In short, media equal real life [24]. A simple example from the book illustrates the point. A kindergarten teacher has a TV with an image of a bag of popcorn sitting on a table. Several kernels have fallen from the bag. The teacher asks what will happen if she turns the TV upside down. Several students respond that the rest of the popcorn will spill out of the bag [24].

The media equation is counterintuitive. It competes with ideas about media that seem much more obvious. Media are tools that help people accomplish tasks, learn, or entertain themselves. People are aware that media are tools. People do not have social relationships with tools. However, Reeves and Nass conclude that people respond socially and naturally to media even though they believe it is not reasonable to do so.

The theory of the media equation extends beyond an intuition that protests: "Not me, I know a picture is not a person." Reeves and Nass argue that the media equation applies to people even though they do not believe it does. Their point is related to the "not me" syndrome of Philip Zimbardo [24], who argues people often believe that their attitudes and actions are not subject to outside influences. This is a particularly dangerous belief because ignoring the power of outside influences makes us more vulnerable to them.

People in the context of the media equation are the selective universal qualifier. The media equation is presumed to be equally applicable to everyone. The theory that all humans, by default, associate media with real life reinforces an assumption that rules we apply to everyday social interaction with each other in the physical world are equally applicable to comparable interactions in the virtual world [22], [25].

The authors of The Media Equation suggest that this is the product of the slow evolution of the human brain relative to technology evolution. Our brains have evolved from a time when only humans exhibited social behavior and all perceived real objects were physical objects. So, when modern media engages old (read: slow to evolve) brains, it is difficult to overcome our hardwired default tendency to assume that mediated presentations are real [24].

People do not naturally scrutinize their actions or their environment and live their lives with little introspection. When our brains respond to characteristics of media or the situations in which they are used, there is little to remind us that the experience is not real. Without some interruption or obvious warning that we have been fooled, our brains will accept media as real people and places [24].

For example, when watching a horror movie in a movie theater and there is a scary scene, a person will be scared and startled first, and consciously acknowledge “it is only a movie” second. IVEs are particularly well suited to apply this idea because the environments are constructed to look and feel very similar to the physical world. The experience is intended to fully immerse the user and reduce or eliminate outside stimuli. Interactions with other users in the virtual world take place through controlled interaction of avatars. It is important to remember that there is a real human being behind every avatar. The people are very real. It is just the medium that is different. The avatars are visual representations of humans. There is very little in an IVE to trigger a mental reality check where a user would temporarily acknowledge he was not interacting in the physical world. Even if that occurs, there is a sufficient immersion stimulus to quickly draw the user back in.

The research that supports the media equation suggests that even the simplest textural and pictorial material can elicit this response from users. It is not necessary to have the most robust media such as IVE technology. The level of realism and immersive tendencies that IVEs provide should only serve to make it more difficult for someone to consciously think their way around them.

The counter-intuitive notion of the media equation combined with the assumption that social rules apply equally in the virtual or physical world reveals strong potential for the employment of IO in IVEs. The immersive qualities of IVEs as described in Chapter I can converge to promote a comparable counter-intuitive idea; avatars = real people and IVEs = real environments. The characteristics of the interaction are more prominent in the user’s mind than the reality (read: artificiality) of the situation. A simple way to conceptualize this is to consider the interactions of small children and Muppets on Sesame Street.

Often interactions on the show are executed to put forth a message; be nice to others, do not talk to strangers, etc. The children are aware that they are on a TV set and that people are manipulating the Muppets. But the children interact with the Muppets directly and perceive them as real. Further, they are able to be influenced through these interactions. This illustration suggests that people can be influenced through direct interaction with (media). Behavioral research specific to Human-Computer Interaction (HCI) supports this conclusion.

5. Captology

> Captology - the study of computers as persuasive technology - focuses on Human-Computer Interaction (HCI), not on Computer-Mediated Communication (CMC). Specifically, Captology investigates how people are motivated or persuaded when interacting with computing products rather than through them. [26]

In 2003, Dr. B.J. Fogg, leader of the Stanford Persuasive Technology Lab, published a book based on his Captology research [26]. As indicated above, Dr. Fogg's research examines how people's attitudes and behaviors change as a result of interacting *with* computing technologies. Figure 6 illustrates that Captology research includes many different computing technologies or platforms and each is capable of affecting influence. For the purposes of this thesis emphasis is placed on IVEs but comparable IO utility may be possible through the other computing technologies listed.

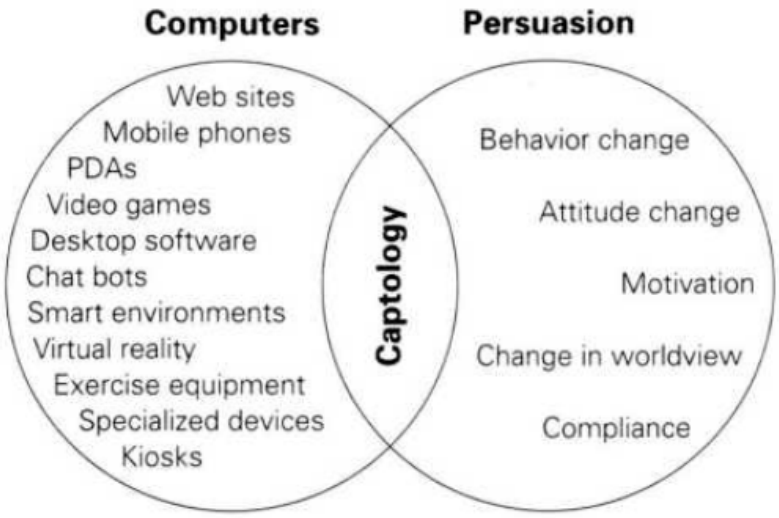

Figure 6. Captology Focus. From [25]

In his book, Dr. Fogg suggests that the easiest way to introduce Captology is through what he calls the "functional triad." This helps provide a conceptual framework of the different roles that computing technology can play; as a tool, a medium, and as a social actor [26]. Figure 7 introduces these roles.

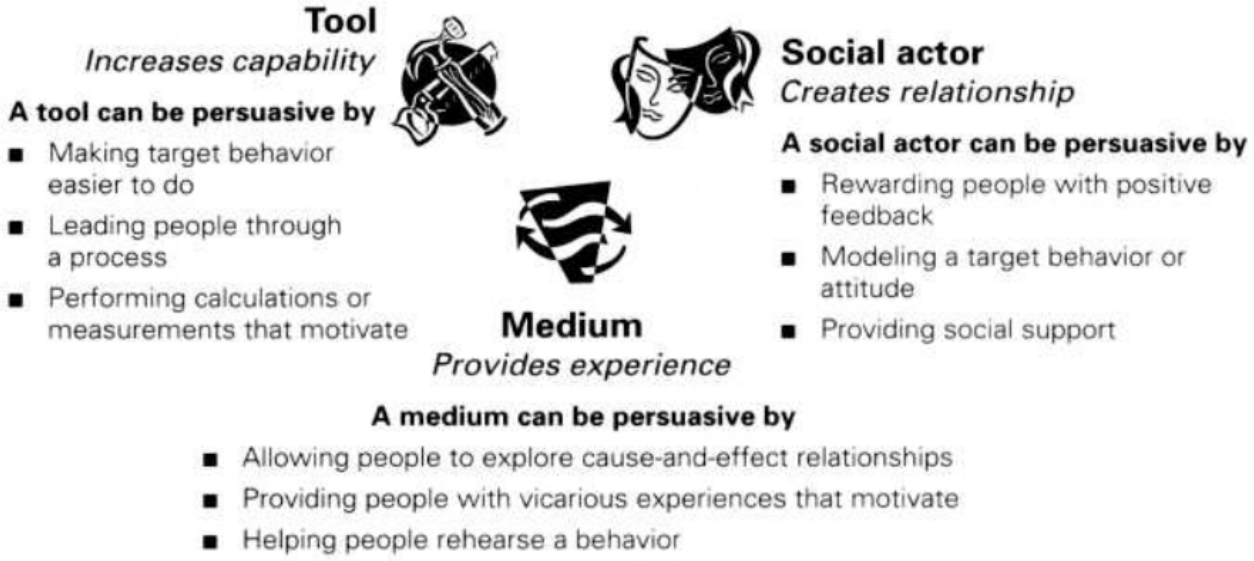

Figure 7. Captology Functional Triad. From [25]

Persuasive technologies can be used as a tool by making complex tasks simpler through a reduction of steps or guiding users through those steps. Consider telephone voice prompts as an example. The voice prompts guide users through options and steps to achieve an end state. A Web-based training tutorial for the installation of a computer program is another example.

Or the technology could be specifically tailored to the needs, interests, of the individual or other relevant factors. Persuasive technologies can offer suggestions to users regarding courses of action based on specific criteria or evaluation of input. The user interface for Amazon.com is a good example of this type of persuasive technology. When you view an item, you are also provided links to related items. The site also makes suggestions for alternate items based on your recent searches.

In *Second Life,* the Residents have the ability to own property and build anything they want. In the context of a Captology tool, an adversary could create an environment or element of one that offered this type of persuasive assistance [26]. For example, he might create an interactive map for newcomers that made suggestions on how to best explore the world. The map would provide positive feedback for movement toward specific areas and discouragement for moving away from them.

As a medium, computing technologies can suggest different pathways to persuasion through simulation. The simulations do not specifically need to force ideas on users. Instead, they offer a safe environment where cause-and-effect scenarios can be explored with relative safety and without fear or judgment, injury, or retribution. The U.S. Army developed *America's Army* based on this idea. *America's Army* is an online team-work based, multiplayer, force-on-force simulation game that allows players to explore Army life from basic training to combat missions without actually requiring a military obligation or enlistment [27].

America's Army is not an IVE, per se. It is more appropriately characterized as an MMORPG because interaction in the environment is goal oriented and the world has finite boundaries. Still, it fits within the scope of a computing technology and, therefore, retains applicability for illustrating computing technologies as a medium.

Game players in *America's Army* can experiment with different strategies for mission accomplishment without the possible consequences normally associated with combat operations. For example, where a failed mission in Iraq would likely result in lives lost, the only consequence of a failed mission in an *America's Army* mission would be the hassle of having to start over. The freedom to explore cause and effect scenarios allows people interacting in IVEs to make bold choices and engage in more risky behaviors than they would in the physical world because there is no tangible physical risk involved.

Computing technologies can also act as social actors, persuading people to change attitudes and behaviors by providing social support, modeling attitudes and behaviors, or leveraging social rules and dynamics [26]. It is within this last category that computing technologies prove most relevant.

As mentioned, *America's Army* allows players to explore Army life. In this context, *America's Army* can be considered a social actor. Beginning in boot camp, military training establishes social dynamics, hierarchy, and defined roles through regimented schedules, a finite rank structure, and incentives for appropriate behavior or responses. Combat training includes psychological conditioning to enable individuals to operate in high stress situations. Over time, this allows individuals to develop relationships with the environment and individuals within it. Relationships lead to familiarity. Familiarity leads to trust. Trust leads to influence.

The utility of Captology is predicated on the assumption that individuals view avatars = real people and IVEs = real environments. Specifically, the characteristics of the interaction with the technology are most prominent in the user's mind. However, this assumption may not be absolute. Users may acknowledge the implied human presence and view the IVE and avatar as communication mediums rather than actual entities. In that case, IVE utility is realized through Virtual Human Interaction (VHI).

6. Virtual Human Interaction

The Virtual Human Interaction Lab (VHIL), located at Stanford University, is focused on human-human interaction through technology. In 2004, Dr. Jeremy Bailenson

(et al.) published a paper that introduced Transformed Social Interaction (TSI) [22]. TSI evaluates the impacts of strategic decoupling of verbal and non-verbal communication that occurs within what they termed to be Collaborative Virtual Environments (CVE) [22]. This thesis, as in Scharlat's work, will use the term IVE to denote both CVEs and IVEs.

Communication between two or more people can be loosely defined as the transmission of some information between the parties using a combination of verbal (talking) and non-verbal expressions (body language). In the physical world, it is difficult to decouple body language from the spoken word [28]. For example, experienced police officers are able to detect deceit when interviewing suspects based on body cues, such as fidgeting or gaze aversion despite the suspect's verbal assertions of innocence [28].

In contrast, virtual worlds provide opportunities to either couple or decouple non-verbal communication with verbal communication through manipulation of a user's avatar and the environment. The author identifies three dimensions of TSI: sensory abilities, situational context, and self-representation [22]. Through manipulation of these dimensions, users can strategically alter the aspect of the conversation in order to achieve the desired result.

a. Sensory Abilities

Sensory abilities deal with our ability to capture data about our environment[9] and actions occurring within it. Consider a distance learning environment as compared with a traditional classroom environment. In a traditional classroom, the teacher can observe the room and each student, immediately evaluating their attention span, level of comprehension, and so on. In a distance learning environment, the teacher only has that capability relative to the students physically present in the classroom. There is limited capacity to evaluate the required metrics for geographically dispersed students.

If that same distance learning environment were located within an IVE, tools could be used that provided the teacher with real-time summary information about

[9] The authors are referring to the virtual environment as opposed to the physical environment.

the attentions and movements of all student interactants [22]. In this way, the teacher could receive the same feedback and situational awareness possible in a traditional classroom.

b. Situational Context

Situational context can be used to transform the spatial or temporal structure of a conversation. In the aforementioned distance learning example, each user in the IVE can optimally configure the geographical setup of the room such that each perceives they are sitting in the front of the room and the rest of the students are sitting behind them [22].

Arguably, comparable sensory ability and even the described situational context scenario could be provided in a distance learning environment supported by Video Tele-Conferencing (VTC), through Webcam distributions, and similar systems. However, those technologies fall short of being able to provide the final dimension of TSI: self-representation.

c. Self-representation

Self-representation has been identified as perhaps the most powerful and applicable TSI dimension [3]. It deals with the strategic decoupling of the rendered appearance or behaviors of avatars from the actual appearance or behaviors of the human driving it. This could be accomplished manually or through digital automation. In the distance learning example, the teacher could tailor the appearance of his avatar to best maximize attention and learning. It could be that some students prefer a smiling teacher where others prefer to have a serious, pensive teacher. Gender, ethnicity, and other student specific preferences could be tailored to optimize the learning environment for the student [22]. Each student would see a unique rendering of the teacher's avatar based on that student's specific preferences, characteristics, or perceptions. In [22], self-representation is broken down into three sub-categories, morphing, mimicry, and Non-Zero Sum Mutual Gaze or NZSMG.

(1) Morphing. Morphing incorporates the recognizable features of one avatar to another. An avatar could be made to look more like the target

being interacted with, or someone that the target finds trustworthy. In this way, an avatar can be perceived as becoming or being more attractive. Research shows that attractiveness felt by a target avatar translates to trustworthiness, ultimately leading to influence. This is an extremely important and powerful capability. An avatar could be patterned after a favorable and likable representation of a Middle-Eastern man with specific attributes taken from existing avatars. That avatar could interact with other Middle-Easterners in *Second Life* and promote and generate pro-U.S. thoughts and ideas. Those ideas would be transferred to the humans behind the avatars and convey into the physical world, thereby increasing pro-U.S. thought and perception in Middle-Eastern regions.

(2) Mimicry. Mimicry, also known as the chameleon effect [22], is very similar to morphing and possesses similar influence potential. Mimicry works by subtly mimicking actions of the target avatar. Like morphing, this leads to the avatar being perceived as more attractive, ergo, trustworthy. The avatar could be made to mimic certain body movements or customs shared by a target demographic, such as bowing to greet an Asian avatar. Incorporating customs that individuals are familiar with and comfortable with will set them at ease and help to gain trust.

(3) Non-Zero-Sum Mutual Gaze (NZSMG). This is a unique capability not possible in the physical world. An individual speaking in an auditorium cannot make eye contact with every person in attendance at once. The speaker's gaze must be shared among all participants in some percentage where the sum cannot exceed 100%. In IVEs, a speaker can be perceived to be providing 100% gaze to each and every member of the group. The perception can be given that the speaker is talking directly to each person. The perception of undivided attention does not necessarily lead to likability, but it does have an effect on memory recall and enhanced learning [22], which could provide enhanced benefit when attempting to convey IO messages.

E. CONCLUSION

IVEs are a real and pervasive trend in cyberspace today. Their use spans social interaction, business use, marketing, and politics, as well as military simulation and training. IVEs are changing the way humans interact and communicate in both social and

professional settings. They link users from around the globe in common environments that transcend traditional national boundaries and geography.

The persistence and future of IVEs is underscored by the real economic impact they have in the physical world. The economies of these environments and their effect on the physical world will undoubtedly drive further investment and growth. IVEs and their economic impact on the physical world will only continue to grow. This trend shows no sign of decline.

IVEs must be viewed as potential operating environments. Users can become immersed in them to a point where the distinction between virtual and the real world is blurred and not distinguishable. Short of biological functions, users can do almost anything in an IVE that they do in the real world. Yet, very few users expect to be the target of IO in an IVE. Despite the level of immersion, there remains a sense of game-like feel. Within this game-like environment, the avatars around you appear innocuous and benign. There exists no obvious reason to maintain a heightened sense of security.

A paradigm shift within DoD must occur in order to change the perception of IVEs from simple novelty game spaces to robust operational environments with real social and economic impact. From this shift, a clearer view of the opportunities and vulnerabilities associated with the conduct of IO within IVEs can be appreciated. Failure to recognize and respond to the impact IVEs creates a seam and critical vulnerability that our adversaries will be quick to exploit.

THIS PAGE INTENTIONALLY LEFT BLANK

III. IMMERSIVE OPERATIONAL RELEVANCE OF IVEs

A. INTRODUCTION

The previous chapters presented information intended to provide background to inform the reader on the concepts of cyberspace, IVEs, and IO. Also presented was an introduction to research centered on the social interaction of humans and computers. This chapter will build on that foundation and establish the operational relevance of IVEs to IO.

B. IVE BATTLESPACE

Identifying where IVEs fit within the information environment is a necessary precursor to determining the existence or extent of IVE operational relevance to IO. Figure 8 depicts the current categorization of the information environment [2]. IVEs exist predominantly in the cognitive dimension. This is where IVEs present the greatest opportunity for influence through IO. From [2], "The cognitive dimension encompasses the mind of the decision maker and the target audience (TA). This is the dimension in which people think, perceive, visualize, and decide."

IVEs also exist in the informational dimension. IVEs have relevance to the content and flow of information within this dimension. This relates to conveying the right message at the right time and presenting the right look for the avatar at the right time and to the right audience.[10]

The physical dimension "is composed of the command and control (C2) systems, and supporting infrastructures that enable individuals and organizations to conduct operations across the air, land, sea, and space domains. It is also the dimension where physical platforms and the communications networks that connect them reside" [2].

[10] In Chapter II, the concepts of morphing and mimicry were discussed—the ability to change an avatar's appearance.

Because IVEs exist in Cyberspace[11] and are software-based systems with no significant physical infrastructure, they have limited operational relevance in the physical dimension.

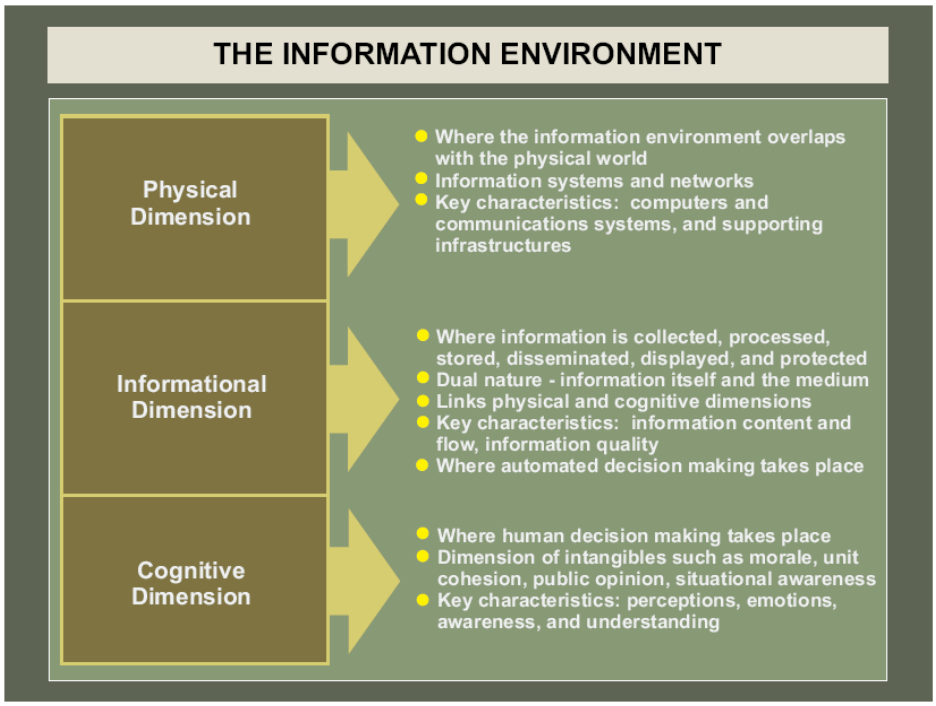

Figure 8. The Information Environment. From [2]

C. IVES ARE PERVASIVE TECHNOLOGY

Pervasive connective technologies surround our daily lives and allow almost instant access to anyone on the planet. As the Dodds study in 2003 demonstrated, the Internet and related technologies have enabled humans to connect with each other on a global scale and at ever increasing speeds [20]. Written correspondence can be sent around the globe in seconds via chat programs or Email where postal carriers once took days. Voice over IP (VoIP) communication can take place in real-time at reduced cost compared with conventional cellular or land-based telephone systems. Pervasive connective technologies are enabling humans around the world to be more connected than ever before, and this trend continues to grow [19].

[11] As of the writing of this thesis, Cyberspace has not yet enjoyed general acceptance as a separate and distinct warfighting domain. Cyberspace must be viewed as a fifth operational warfighting domain in order for the full potential of IVE exploitation to be to be realized.

Consider an individual who wants to have a custom home built. Before IVEs, the home buyer would physically meet with an architect to discuss the design. Revisions and design changes would be communicated through voice and data communications. In a best-case scenario, the architect would have CAD software that would allow him to provide a 3-D rendering that the home buyer could view. Unfortunately, the rendering would only be available on the CAD computer on which it was designed, so the home buyer would have to travel to the architect's office again to view subsequent iterations of the design.

In contrast, the architect could have created the design plans in an IVE. This would allow the home buyer to view the plans remotely (wherever he had access to the Internet). With a rendering built within an IVE, the home buyer could walk through a completed virtual representation of his new home, fully furnished, using his avatar. This would provide the home buyer confirmation that the home fit his needs before the construction begins. Additionally, since the IVE is independent of physical geography, the architect and home buyer need not physically meet until the final plans were confirmed and the purchase took place.

Immersive Virtual Environments represent the next generation of pervasive connective technology. IVEs can provide users with comparable collaborative and communicative capability that exists with chat, email, video-teleconferencing, and physical human interaction. Unlike its predecessors, an IVE can combine all of those capabilities and provide them through an interactive 3-D environment that has the same look and feel as the physical environment of the user.

Chapter II provided some metrics for *Second Life*. In particular, Figure 2 showed the current number of Residents of *Second Life* has reached 19 million. Figure 9 shows demographic summary information of those Residents [13]. Usage hours by gender were slightly skewed, with roughly 60% male. The important observation is that interest in IVEs is not exclusively a youth-based phenomenon, but spans all ages.[12]

[12] *Second Life* is an adult's only community (18+).

Usage hours by Age Band	
	% of Total Hrs
13-17 (Teen Grid)	0.53%
18-24	15.53%
25-34	34.77%
35-44	28.28%
45 plus	20.37%
Unknown	0.51%
Usage hours by Gender	
Male	59.57
Female	40.43

Figure 9. Demographic Summary Information: Age and Gender. From [12]

Individuals are not alone in assessing and exploiting potential benefit and use of IVEs. Universities are using IVEs and establishing virtual campuses. There are nearly 100 academic organizations listed in the *Second Life* Education Directory [31]. Among them are functioning virtual campuses for Ohio University, University of Delaware, Washington University, University of Arizona, and Texas A&M University, to name a few [29], [30], [31]. Figure 10 shows the entrance to the Ohio University virtual campus.

Figure 10. Ohio University Virtual Campus, viewed from above. From [28]

Many businesses and government agencies have also begun to show interest and have invested time and money into future development in *Second Life* [32]. For example, reference [32] suggests that enterprise customers are using *Second Life* as a collaborative tool that rivals Cisco's Telepresence.[13] Online collaboration and meetings are a large draw for these businesses and organizations. The president of the IBM Academy of Technology commenting on the success of a virtual meeting in *Second Life* said, "The meeting in *Second Life* was everything that you could do at a traditional conference—and more—at one fifth the cost and without a single case of jetlag" [34].

Reference [35] provides a more comprehensive list of how businesses are using *Second Life*. Capabilities include, but are not limited to, product sales, virtual meeting spaces, human resource recruitment, marketing, simulation, and research collaboration. Reference [35] provides two lists. The first is comprised of businesses and organizations that are legally registered or recognized entities created specifically for *Second Life*. The second list contains those businesses and organizations originating in real life that have operated in *Second Life* and were not founded specifically for *Second Life*, but have involved themselves in the world.

A timely development relative to this thesis, the USAF issued a Request for Proposal (RFP) in early September 2008 that seeks to create an IVE that is an "interactive virtual representation of an Air Force base to provide a distributed learning environment" [36], [37], [38].

The USAF RFP demonstrates a long-term outlook to the benefit of IVEs. Two important points should be recognized. First, that a DoD component has recognized long-term benefit from the integration of IVEs for the training and development of their personnel. Second, there is an acknowledgement that interactions in virtual worlds can and do have meaning and influence in the physical world. The latter will be discussed in greater detail in the following section.

[13] Cisco TelePresence combines high-quality audio, high-definition video, and interactive elements to deliver an in-person meeting experience over your network [32].

D. INFORMATION OPERATIONS WITHIN IVES

The foreword of the National Defense Strategy of the United States of America 2005 [39] makes a distinction between the challenges the nation faces today and those that were faced by the defense establishment during the Cold War and prior. In the foreword, former Secretary of Defense Donald Rumsfeld makes clear that there is fundamental importance in influencing events before the challenges we face grow more dangerous and less manageable. The 2005 National Defense Strategy stresses the importance of Information Operations becoming a core military competency, as successful military operations depend on the ability to protect information infrastructure and data. JP 3–13 [2] describes IO as the integrated employment of core, supporting and related capabilities designed to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own. Both publications make reference to the importance of leveraging influence to achieve success in military operations through the use of IO.

IVEs possess unique characteristics that make them obvious conduits for the employment of IO capabilities to effect influence in the cognitive domain. These characteristics manifest themselves as both opportunities and vulnerabilities. For illustrative purposes, employment of these characteristics are thought to target civilian populations in an effort to influence public opinion, but could easily be adapted for use with any inhabitants of virtual worlds.

1. Access

IVEs exist in cyberspace. Transcending geographical boundaries, these worlds provide the potential to engage in face-to-face interaction (through avatar engagement) with anyone on the planet. Further facilitating global reach are language tools. These might allow an English-speaking person to have a real-time conversation with a non-English-speaking person and vice versa. Neither person need know a second language. Neither person may even be aware that different languages are being used. Each user perceives the conversation is taking place in their native language. Translation

tools within the software remove language barriers that would preclude effective communication in a conversation that took place in the physical world.

An assumption that must be verified to ensure accurate conveyance of intended communication is that translation tools provide correct translation of messages. Most, if not all, of these language tools are automated and may not be programmed to catch subtle differences in translation of key words. The possibility therefore exists for unintended effects resulting from poorly translated IO messages.

2. Anonymity

Avatar creation capability in IVEs is unlimited. An avatar can be made to resemble a specific person or made to appear common and ambiguous. The appearance can be altered when necessary or desired through simple modifications. Modifications or changes to an avatar's appearance can be fine-tuned to support intended IO effects. The concepts of morphing and mimicry introduced in Chapter II are prime examples of how this could be accomplished.

3. Method of Delivery

In an IVE, an avatar can provide information through face-to-face virtual interaction. Preconceptions and bias toward media organizations, printed media, and other sources of information can be overcome. Avatars can disseminate information through "word of mouth" that carries an inherent believability because it was provided by a (virtual) person vice a news organization, government organization, or political figure.

Another method that could be exploited in IVEs surrounds land ownership. In *Second Life* and other IVEs, users can buy land, commonly referred to as "islands." These islands can be made public or private and provide as much or as little access as required. An island could be constructed around a specific IO intent in its entirety, or elements of that island (or any part of an IVE space that can be modified) can be tailored to the specific message or intent. For example, the United States could create an island that provided visitors a U.S. perspective of the conditions in Iraq or Afghanistan. Virtual billboards of presentations could be provided to show the positive affects U.S. presence

in the region has had. U.S. public affairs personnel could control avatars on the island. Those avatars could provide scripted messages, presentations and explanations of information, as well as answers to questions and gauge reception of the content and suggest changes based on visitor feedback.

E. CONCLUSION

IVEs are powerful environments that generate real human responses through real human interaction. The impact of interaction in these environments transcends the virtual environment and has measurable social and economic impact in the physical world. Interest and participation within these environments is growing. IVEs nullify traditional boundaries of geography, nations, culture, and politics. There is great potential to leverage IO within these environments, targeting the cognitive domain to achieve influence and intended effects. IVEs present unique and evolving opportunities for the use of Information Operations. They simultaneously expose potential vulnerabilities if these opportunities are leveraged against our own nation or military. To ignore IVEs or dismiss them as games or something equally benign is a dangerous prospect and understates their value and importance in today's society.

IV. CHINA

> Contemporary threats share an important characteristic with past threats. A timeless and fundamental principle of the profession of arms is to avoid the strengths and focus on the vulnerabilities that will most rapidly and decisively cause the opponent's defeat. The capabilities of American military power make it difficult for any adversary to develop a symmetrical force that mirrors that of the United States. The Armed Forces of the United States must, therefore, expect adversaries—whether states or nonstate groups—to seek to exploit asymmetries and focus on U.S. vulnerabilities. Combatant commanders must anticipate asymmetric threats in preparing for and conducting joint, multinational, and interagency operations. [40]

A. INTRODUCTION

In keeping with the principles of China's classic military strategist, Sun Tzu, two senior People's Liberation Army (PLA) colonels propose "using the inferior to defeat the superior" and "winning the war without bloodshed." In their book, *Unrestricted Warfare***,** Qiao Liang and Wang Xiangsui propose a series of asymmetric strategies for securing China's dominance as a global power [41]. *Unrestricted Warfare* suggests that China is unlikely to challenge the United States with conventional kinetic methods. Instead, China will employ an offensive style of warfare that surpasses all conventional boundaries, ethics, and concepts of war to topple America's dominant influence in the world. The exploitation of IO in IVEs certainly qualifies as surpassing conventional boundaries and ethics. This chapter will examine the potential for IO exploitation of IVEs by China against the United States.

B. CHINESE DOCTRINE

Sun Tzu said, "If you know your enemies and know yourself, you will not be imperiled in a hundred battles." It is a far simpler task of knowing yourself. We are predisposed to evaluate based on our own thoughts and ideas. It requires a greater effort to put yourself in the mind of your adversary. This effort must be undertaken to adequately assess the risk associated with China's potential use of IO in IVEs. The origins and foundations of Chinese military thought surrounding asymmetric warfare and

IO are introduced below in order to illustrate why it is plausible, if not probable, that China could employ this type of IO campaign, particularly against the United States. The most illustrative influences to China's IO/IW mindset appear to be those of Sun Tzu, Mao Zedong, and Liang and Xiangsui's recent book *Unrestricted Warfare*.

China's modern asymmetric warfare strategies toward the United States were developed primarily to deter or delay a U.S. response in Taiwan Strait scenarios [42]. However, they have origins deeply rooted in Chinese historical warfare doctrine. Sun Tzu's writings in *The Art of War* have had a tremendous impact in Chinese political and military thought throughout its history and continue to do so.[14] From Sun Tzu's writing came the emphasis on attacking psychology vice physical forces, attacking an enemy's strategy, avoiding enemy strong points, and the use of deception and pre-emption.

Mao Zedong's most relevant contribution to Chinese military strategy, and this thesis, is the concepts of the People's War. Though Mao Tse-Dong claimed he never read *The Art of War*, his concept of the People's War was deeply influenced by Sun Tzu [43]. From the Chinese perspective, the People's War embodies the idea of overcoming the superior with the inferior.

Unrestricted Warfare, literally translated "warfare beyond bounds," was written in 1999 by two Colonels in the People's Liberation Army (PLA). In the book, the two PLA authors discuss twenty-four different "military," "transmilitary," and "nonmilitary" strategies. In modern warfare, all of these strategies could be combined and practiced for the single purpose of defeating an enemy without incurring significant loss of personnel or equipment. The book describes how this defeat is possible through a number of alternatives to direct military confrontation. One of these alternatives is network warfare. It is in the area of network warfare that IO in IVEs is most likely relevant.

An *Unrestricted Warfare* review essay written by Cheng Dean suggests that the book has aroused significant debate in both China and the United States. Some believe

[14] The influence of *The Art of War* extends well beyond Chinese military theorists. It has become popular among military theorists world-wide as well as political leaders and those in business management. This is because the book approaches strategy in a broad fashion, allowing for adaptation of its concepts across management, administration, and planning in addition to the obvious military context.

the book represents a virtual blueprint for how China will fight future wars. Others speculate that the book is simply an opinion piece written by two mid-level officers. What was not in debate was that the book has been widely read. According to [44], the initial print run of 3000 copies quickly sold out. Five subsequent editions were printed and sold; the book achieved bestseller status in China with 40,000 copies. Of particular note, the book was read with great interest by then Chinese President Jiang Zemin and Minister of Defense Chi Haotian. The book remains in high demand with translated copies available worldwide.

C. IO FROM AN ASIAN PERSPECTIVE

In the same fashion that Chinese military doctrine must be understood from their perspective, so too must their concept of IO be examined in context. Throughout this thesis, IO has been referenced in terms of the Western sense of information operations as defined by JP 3–13. To impose our interpretation of IO on China would be a mistake. There are significant and key differences that must be considered when assessing China's use of IO. One important distinction between eastern and western interpretations is that China does not view IO as confined solely to military operations [43]. Another significant difference between Eastern and Western interpretations of IO is that China does not view IO activities as support tools or force multipliers but rather as primary attack tools or critical weapons to employ against more advanced states.

Part of the reason for China's interpretation of IO as a primary weapon versus a supporting arm or supplemental tool was born out of observations of the fall of the Soviet Union. The Chinese learned a valuable lesson related to the futility of attempting to match U.S. defense spending in an arms race. At the same time, China observed that U.S. strength hinged on effective and extensive C4ISR use. This strength was simultaneously seen as a vulnerability that could be exploited through IW/IO [43]. In testimony before the U.S.-China Economic and Security Review Commission in 2005 [45], James Mulvenon provided more insight into Chinese views of IO in general and CNO in particular.

During his testimony, Mulvenon said the Chinese view IO and CNO as useful supplements to conventional warfighting capability. They provide powerful asymmetric options for "Defeating the superior with the inferior." One PRC author referenced was quoted, "Computer Network Attack (CNA) is one of the most effective means for a weak military to fight a strong one." Another commented on the use of CNO as the spearhead of a deterrence strategy. Through the use of CNA, a message could be sent to the enemy that essentially says, "Don't even try it," forcing them to give up without a fight [45].

While the possibility exists that sending a clear message to adversaries will discourage specific actions, it is also believed that CNA carries with it a level of plausible deniability. Coupled with the plausible deniability characteristic, a successful attack could deliver a paralyzing blow to an adversary who would not be able to determine if the attack came from a simple prank or from a deliberate targeted attack [45].

Drawing inspiration from Mao Zedong's theory of a long protracted war, Chinese CNA focuses on disruption and paralysis of the enemy vice destruction. The intent being to raise the cost to an unacceptable level, erode popular support, and change the perception of the ability to win. CNA has the ability to derive disproportionate effects analogous to the effects of a sniper on the battlefield. A sniper has the ability to hold up a large enemy force by stalling a segment of that force or by shooting a key individual. The resultant loss of momentum of the larger force can convince decision makers it is too costly for the larger force to continue the fight [46].

One of the most significant distinctions between eastern and western interpretations is that unlike the U.S., which views IO as a tool to employ as a force multiplier through all phases of conflict, the Chinese view IO as a pre-emptive asymmetric weapon that must be employed during the opening phases of an operation.[15] This is because the Chinese believe that once conflict is initiated, the enemy may simply unplug the targeted network assets or secure vulnerabilities effectively, obviating prior intelligence preparations of the battlefield. Additionally, China sees this early

[15] In particular, China uses CNA not solely in the conventional sense of attack but also as a probing tool and prep of the battlefield/shaping tool. Hacking efforts by the Chinese identify vulnerabilities or gaps in U.S. cyber defenses and computer networks that can be exploited at a future time and place.

employment of IO as a tool that may preclude the need for subsequent conventional military action.

It is in this mindset of the early employment of IO to fight and win an information war and prevent the need for subsequent conventional military action that IO in IVEs has utility. The use of IO in IVEs can be used in concert with, or in lieu of CNA efforts. Effectively employed within IVEs, IO has the potential to provide influence that may go one step further than CNA. Rather than preparing for an attack or unfavorable action from an adversary, like CNA does for the Chinese, employment of IO in IVEs could prevent an adversary from getting to the point where action is taken. For example, by influencing the opinions, perceptions, and preferences of the U.S. public, an enemy could prevent the U.S. government from taking particular action because of the lack of public support. This employment methodology is directly in line with Sun Tzu's emphasis of attack enemy psychology rather than physical forces [43].

D. NATURAL ADVANTAGES

1. The People's War

The People's War is a military-political strategy created by Mao Zedong. The basic concept behind the strategy is to maintain the support of the population while drawing an enemy deep into a protracted conflict where the population will utilize a combination of mobile and guerrilla warfare to reduce the enemy's forces and their resolve to fight. Chinese theorists believe that a modern application of Mao Zedong's theory can be applied using capabilities and qualities of the information era [47]. IVEs may represent a battlespace in which China can maintain support while engaging the U.S. in an online "Cyber-Guerrilla" war.

Some Chinese theorists believe information engineers will become heroes like the warrior class of the past. They envision a smaller military force augmented with a contingent of information engineers and citizens with laptops who would wage a "take home battle." They have witnessed other countries integrate nonmilitary individuals and groups for execution of IW functions and are keen to point out the role of civilians in IW operations [47]. These nonmilitary groups and individuals are "independent

confederation(s) of patriotic youth dedicated to defending China against what (they) perceive as threats to national pride" [48].

To fully appreciate the people's war concept and the natural advantage it provides to the Chinese, one must shed cultural bias inherent in viewing the idea from a U.S. paradigm. In Chinese society, citizens are an integral part of Comprehensive National Power[16] and a vital component to national security. The Chinese population is factored into China's strategic calculations and will be actively employed equally during war and peacetime.

It is difficult to conceive of the powerful links being formed between state authorities and quasi-freelance IW or intelligence operations because it does not fit the preconceived notion of the proper relationship in Western Democratic societies. It is highly unlikely we would assign such roles to nongovernmental citizens. Title 10 restrictions and elements of the law of war preclude our integration of the U.S. civilian population as combatants. In contrast, the PLA is not constrained by laws and emphasizes the integration of military and civilian roles in their strategic doctrine of future wars:

> In the high-tech local war which we will face in the future, the role of the masses as the main body of the war is embodied by the country. The great power of the people's war is released through comprehensive national power, the combination of peace time and war time, the combination of the military and the civilian, and the combinations of the war actions and the non-war actions. Besides the direct participation and cooperation with the army's operations in the region where war happens, the masses will support the war mainly by political, economic, technical, cultural, and moral means. [49]

The Chinese are able to leverage a broad informal network of students, tourists, teachers, and foreign workers inside a host of nations. Each voluntarily provides small bits of seemingly innocuous information out of a sense of civic duty and national pride. These bits of information, when brought together, form a composite picture of the

[16] The combined overall conditions and strengths of a country in numerous areas. During the Cold War, a nation's power was largely determined by military force. However, as the world moves toward multipolarity, elements such as economics, science, and technology have become increasingly more important in the competition for power and influence in the world [47].

environment. IVEs provide members of these informal networks prime opportunities to demonstrate their national pride.

2. HiPiHi

China's equivalent to *Second Life* is a similar IVE called *HiPiHi*. Development of *HiPiHi* began in 2005, with a mainstream release to the global public in March 2007 [50].[17] *HiPiHi* is so similar to *Second Life* that there is speculation that the Chinese IVE is essentially a pirated version of *Second Life*. This is very probable, since the Chinese have a history of stealing and reverse engineering various technologies [50]. *HiPiHi* creators suggest coincidence and concurrent development as an explanation for the similarities and relatively close timelines.

Regardless of the origins, China gains unique and significant strategic advantages through *HiPiHi*. The site is purported to be "created, inhabited and owned by its residents. The residents are the Gods of this virtual world; it is a world of limitless possibilities for creativity and self-expression, within a complex social structure and a full functioning economy" [52]. While this may have been the original intent for *HiPiHi*, the Chinese government is known to censor content. Recently, Google agreed to provide a Chinese version of its search engine that will censor search results to satisfy government in Beijing [53]. Similar strategies are employed in *HiPiHi*. While cybersex in *HiPiHi* is considered acceptable as long as it is done in private, political discussion is strictly prohibited [54].

Virtual geography is another part of *HiPiHi* being regulated. The IVE is being segregated by region. Parts of *HiPiHi* are restricted to Chinese only. Americans and Japanese have their worlds hosted on separate servers hosted in their countries and movement within *HiPiHi* is generally restricted to their parts of the globe [54]. There is the potential to exploit this segregation as an IO tool. As mentioned in the Virtual Human Interaction section of Chapter II, virtual worlds provide opportunities to strategically alter aspects of the interactions between avatars or the environment to achieve a desired result.

[17] Although the debut was globally available, the application, all documentation and language was in Chinese only, with interface English translations of the "how to use *HiPiHi*" information made available in July of the same year [50].

The example in Chapter II dealt with optimizing the experience for each student in a distance learning environment but could be adapted for any intended effect. Because China has segregated portions of *HiPiHi*, they have the ability to alter aspects of one area independent of another. This provides greater flexibility to tailor messages for intended audience without concern for unintended effects of others in the same space.

Prohibited political discussion and off-limits regions of *HiPiHi* are not the only areas where the Chinese government is providing regulation and oversight. When interviewed in August 2007, *HiPiHi*'s creator was asked about the possibility of *HiPiHi* creating its own currency comparable to *Second Life's* Linden dollar. He responded by saying that there was no immediate plans for the creation of *HiPiHi* currency, suggesting that it was too soon after the launch of *HiPiHi* to definitively answer how or when in world currency might appear [55], [56]. In reality, the Chinese government has restricted virtual currencies out of fear that conversions into Yuan could undermine the country's financial system [57]. Impacting currencies and economies of adversary countries is one of the new concepts of weapons described in Unrestricted Warfare [41].

China could have even greater influence if most of the world was using *HiPiHi* vice Western systems such as *Second Life*. The same information shaping, censorship, oversight, and control leveraged on the Chinese people could be adapted to the global user base. Complimenting censorship efforts, preferred content could be injected or advertised in the IVE. Unfortunately, *HiPiHi* Resident[18] growth does not immediately suggest a great potential for influence. Second Life is still the predominant IVE. In August 2007, Hui Xu, *HiPiHi*'s founder and CEO reported 13,000 residents in *HiPiHi* [55]. The current Resident count has only marginally risen above 100,000 [58]. In contrast, there are more than 19 million Residents in *Second Life* [12]. Still, techniques and methods relating to censorship and information control can be tested and refined within *HiPiHi* and variations later used within *Second Life*.

An examination of *Second Life* user hours by country for third quarter 2009 reveals the United States ranked number one, with 48,741,401 hours [59]. That equates to

[18] As with *Second Life*, a Resident in *HiPiHi* is a uniquely named user.

just over 2.5 hours per U.S. user. China ranked 28th, with 287,288 hours distributed among an estimated 111,785 Chinese *Second Life* residents.[19]

While *HiPiHi* has limited use for influencing the global public due to access limitations, it does offer China a unique advantage. *HiPiHi* could be employed as China's equivalent to a Honeyworld.[20] In this context, *HiPiHi* could be used as a test environment to refine and evaluate IO methods before they are employed in *Second Life* or other IVE.

3. IO/IVE Immunity

The results of a recent comparative study conducted by Queensland University of Technology suggest that Australians might be more susceptible to interactions in IVEs than Chinese [61]. The study investigated the cross-cultural differences between individuals interacting within IVEs. The study measured and compared levels of Presence[21] obtained by Australian and Chinese participants during an IVE session. The results have highlighted that a statistical difference in Presence exists between the two groups; however, no difference in Immersive Tendency[22] was identified [61].

From the Chinese perspective, the results of the study suggest another strategic advantage. The Chinese are less likely to be influenced through interactions within IVEs. This advantage is comparable to wearing body armor in combat; the likelihood of being injured from gunfire is reduced. Chinese (military and/or civilian) could be employed en masse to achieve economies of scale when employing IO within IVEs with decreased

---

[19] (User Hours / Total Residents) = Average User Hours. U.S.: (48,741,401 / 19,000,000) = 2.57 hours. Assuming user hours average as a constant, estimated Chinese users in *Second Life* can be derived by: (287,288 / X) = 2.57 → (287,288 / 2.57) = 111,785.

[20] The Honeyworld concept is described in detail in Ryan Rippeon's thesis, *Clandestine Message Passing in Virtual Environments* [59].

[21] Presence "is an existential phenomenon that is triggered by features of the virtual environment and moderated by user characteristics." In the study, Presence was used to measure differences in the ability to control events within the environment, respond to actions and visual aspects of the IVE, and how involved in the overall experience they became [60].

[22] Immersive Tendency identifies and measures possible individual difference in the ability of a person to immerse themselves in different environmental situations, not just an IVE or virtual environment. Examples include the ability to become involved in books or television, identify with characters within such media, the ability to block out distractions and become engaged with computer games [60].

concern for effectiveness of potential adversarial reciprocation. Similarly, Chinese citizens could participate en masse in IVEs attempting to gain intelligence or to attempt to win hearts and minds with low risk of susceptibility to adversarial intelligence and propaganda activities.

4. Public Opinion and Support

China's War of the People enjoys persistent support of the populace through a perception of a common struggle [48]. China can leverage its public support against America's lack thereof and effect influence in IVEs through the interaction of users. In contrast, America seems to have a short attention span and tolerance for combat operations [62]. By undermining and reducing American public support, the Chinese could force American politicians to acquiesce to public opinion.

There is some debate over the effectiveness of Internet technologies like IVEs being used to foster public opinion and support or being used as political platforms. Technological enthusiasts see great promise in the medium. Skeptics, however, maintain that such technologies will reinforce existing social inequities rather than promote new political subjectivities. In either case, it is undeniable that Internet technologies are open-ended. The effect of their use is dependent on the subjectivity and intentions of their users. The combination of availability and adaptability give these technologies significant potential to foster new forms of politicization[23] [64]. China's ability to subjectively censor[24] content in *HiPiHi* gives them a unique advantage in fostering and maintaining public opinion and support for national policy, ideology, or agenda.

5. Perception of Military Utility

It is highly likely that the Chinese will recognize and exploit the military utility of IVEs before us. Timothy Thomas examined Chinese IO concepts in his book *Cyber Silhouettes* [65]. In his examination, he noted that the Chinese are developing an updated ideology and strategy of psychological warfare. Its strategy would focus on exploiting the

[23] An example of how IVEs are used to effect political influence: During the 2008 U.S. Presidential campaign, Barack Obama established a campaign headquarters in *Second Life* [62].

[24] Both promotion and inclusion of preferred content and the exclusion of prohibited content.

differences between Eastern and Western mentalities. The Chinese believe that modern psychological warfare can help ensure stability and shape national security thinking, and therefore, has greater utility during peacetime than during war. Recommendations for the development of its updated strategy will undoubtedly lead the Chinese to recognize and subsequently exploit the military utility (read: IO) potential inherent in IVEs.

Strengthening the Chinese advantage of the perception of utility of IVEs is our lack of acknowledgement of the same. Within the DoD, IVEs are still primarily viewed as novelty game-like environments. However, there does appear to be an increasing appreciation for the potential of IVEs to support military education and training. In a Request for Proposal (RFP) issued in Sept 2008, the USAF solicited the creation of an IVE to be used as a virtual education system aimed at the public as well as recruits and career Airmen [36].

The Marine Corps is also realizing the benefit of IVEs as evidenced by a recent test of the Future Immersive Training Environment (FITE). FITE is a virtual reality-based training system intended to improve team decision-making skills through a series of realistic scenarios [66]. The Marines who took part in the test were immersed into environments replicating what they would see when deployed. This allowed them to be evaluated based on reactions to situations and signals they may encounter in a real-world mission situation in order to maximize their performance and survival. The Marine Corps' use of IVEs is based on the conduct of combat operations in a virtual environment. But like the USAF, use is still limited to training and simulation.

Despite the acknowledgement of IVE relevance in a training and education context, there is still a lack of understanding or appreciation for potential operational use and benefit offered by IVEs. Research for this thesis yielded limited information to suggest the DoD has identified any tactical, operational, or strategic benefit or risk from the employment of IO within IVEs. A *Washington Post* article quoted U.S. intelligence officials who said they were convinced that IVEs are seedbeds for transnational threats [67]. They go on to suggest that IVEs could become actual battlefields and that the intelligence community has begun contemplating how to use *Second Life* and other similar communities as platforms for cyber warfare [67].

E. INDICATIONS OF A WILLINGNESS TO ENGAGE IN CYBERSPACE

Chinese cyber attacks against U.S. systems have increased significantly since 2005. However, the characterization of all of these events as attacks would not be accurate. It is likely that many of these unwarranted incursions are reconnaissance missions or focused on security vulnerabilities or gaps in our cyber-defenses [68]. These incursions could be used to plant code that provides trap doors or viruses in our systems. These could be activated at a specific time and place to achieve desired results. These reconnaissance measures appear to conform to a Sun Tzu stratagem that says victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win.

This idea of offensive computer attacks is not new. Chinese theorists were discussing offensive computer attacks over a decade ago. In 1999, a book titled *Information War* [69] contained a section called "Conducting Camouflaged Preemptive Attacks." In the book they state:

> To conduct computer surveillance, we can use computer information networks set up in peacetime and enter networks as different users to do the surveillance in an area broader than the battlefield. We can borrow the power of computer experts, especially hackers, to finish computer surveillance tasks . . . it can be seen that using hackers to obtain military information from computer networks is a very effective method. We should be familiar with network protocols and accumulate network intelligence. [69]

In a separate article written in China's *Jiefanguin Bao (Liberation Army Daily),* it was suggested that China may develop a net force or information warfare branch of the military focused on the task of protecting Chinese network sovereignty and the engagement of net warfare. While there was no evidence that any such service had been established, the authors speculated that its eventual creation was highly likely. Elements of the net warfare would include offensive and defensive technologies, scanning and masquerade technologies, and recovery technology. Masquerade technology would assist a person who wanted to dissemble as a commander and take over a net [68].

There are several examples of recent cyber attacks that can be directly attributed to or are highly likely to originate from China. Recent high profile examples include hacking into the Pentagon's Joint Strike Fighter Project files, a spy ring originating in China stealing sensitive data from around the world, and a Chinese attempt to hack Google.

In April 2009, the *Wall Street Journal* [70] reported that computer spies had broken into the Pentagon's Joint Strike Fighter project. Although many details of the attack were not available to include the specific identities of the attackers, sources reported that the attacks appeared to originate from China. The Internet Protocol (IP) addresses and digital fingerprints were known to be of Chinese origin and had been traced to attacks in the past. The spies were able to download sizable amounts of data related to the fighter. Military officials familiar with the matter confirmed the program had been broken into several times.

In early 2010, North American researchers exposed a China-based cyber-espionage ring that targeted computers in the Indian military and elsewhere [71]. The findings were released in a report written by researchers at the University of Toronto's Munk Centre for International Studies, the Ottawa-based security firm SecDev Group and a U.S. cyber sleuthing organization known as the Shadowserver Foundation. The researchers found a global network of botnets[25] that were made to report to servers in China. The researchers also found the location of where the stolen files were stored. The report does not conclude the Chinese government is behind the activity but does infer some collaboration between the government and the offending parties. A co-author of the report questioned motives asking, "Is the buyer paying the thief to go after this stuff, or is the thief doing it themselves because they know they can find a buyer?" In either case the Chinese government benefits from this activity.

In February 2010, the *New York Times* [72] reported on a series of online attacks on Google and dozens of other American corporations. The attacks had been traced to computers at two Chinese educational institutions in China. One of them has close ties to

[25] Groups of computers or computer systems that have had malicious software installed by worms, Trojan horses or other malicious software that allows the botnet originator to control the group remotely.

the Chinese military. Both the Chinese government and the Chinese schools deny involvement in the attacks. Independent researchers who monitor Chinese information warfare admit limitations in determining where an attack originated from due to the distributed approach China takes to online espionage. In the story, James Mulvenon, a Chinese military specialist and a director at the Center for Intelligence Research and Analysis in Washington commented on the difficulties in tracing activity back to the Chinese government. He said that while the United States compartmentalizes online espionage within specific agencies, the Chinese government involves volunteer "patriotic hackers" to support policies and agendas. This makes it far more difficult to trace an attack to a government origin because in some cases it may not exist.

Because of the nature of computer network operations, it is difficult to determine how many Chinese IW reconnaissance or offensive operations have taken place or to determine the actual intent of the same. In spite of the lack of definitive information surrounding quantity and motive, these examples of Chinese reconnaissance and offensive IW are clear indications of China's willingness to engage in cyberspace.

F. SURROGATES

One of China's stratagems is to kill with a borrowed sword. In the context of cyber warfare, this stratagem describes Mao's "People's War" concept applied through the use of patriot hackers. China does not necessarily need to maintain a military or government agency dedicated to cyber attack and defense. In [68], Tim Thomas states there are more than 250 hacker groups that are operating in China. These groups provide quantity in the number of attacks they can generate and quality in the variety and intensity of the attacks possible. Even if attack origins are traced back to China, none of the attacks can be directly linked to the PLA. This gives the Chinese government plausible deniability, which is one of the most significant advantages of this method of employment.

While China denies responsibility for attacks, there is evidence that they are facilitating the education and training of their citizens in fields that would make them prime candidates to take up "cyber arms." In 2005, China had over one million graduate students in universities and research institutions with focus on hardware, grid and

networking research[26] [73]. China maintains one of the highest graduate student populations in the world, second only to the United States.

There are also indications that China is actively seeking hacker talent among its citizens. In 2007, a *Time* Magazine article [74] described the coordinated effort by Chinese-military authorities to recruit hackers to obtain information from computer systems outside China and launch cyber attacks in future conflicts. A competition for hackers was created, with the winner receiving a monthly stipend from the military.

Proof of Chinese government sanctioned use of surrogates or patriot hacker groups is primarily circumstantial, but as each attack is examined, the evidence becomes overwhelming. If not directly coordinating the efforts, at the very least, the Chinese government is complicit toward these attacks.

G. CONCLUSION

China has natural advantages it is aware of, most notably its public support and contribution toward an asymmetric mindset regarding national defense. Its interpretation of asymmetry includes the justification of pre-emptive offensive attacks to discourage adversaries. China recognizes our weaknesses in perception and motivation relating to IVEs as exploitable seams.

China has demonstrated an uninhibited willingness to engage in cyber attacks and is able to exploit the efforts of hacker groups and private citizens to achieve desired results. This form of irregular warfare poses a difficult challenge to the United States because the enemy is not a singular, easily characterized enemy. In conducting irregular warfare, one can neither ignore the enemy nor the population, and addressing them with equal energy and focus is difficult.

From China's perspective, it makes sense to use any means possible to counter America's technological advantages. They understand the potential that cyber attacks have. A weaker force can inflict serious damage on a superior force with a properly timed and precisely defined asymmetric information attack. China's exploitation of cyber warfare capability has launched the equivalent of a Sputnik in cyberspace [74]. China

[26] The research is funded by the government and topics tasked have government aims.

possesses both capability and opportunity to conduct IO within IVEs. It possesses its own IVE that can be used as a Honeyworld with active government oversight. Based on unclassified information available there appears to be no direct evidence to suggest that China has acknowledged the operational potential of this capability. Regardless, the existence of such a capability presents a threat to national security we cannot ignore.

V. CONCLUSIONS AND FUTURE WORK

A. SUMMARY

This thesis focused on the examination of Immersive Virtual Environments (IVE) and their applicability in the conduct of Information Operations. The growing importance of IVEs in society, as well as within the military, was explored. The operational relevance of IVEs beyond that of simulation and training tools was emphasized. Finally, China was offered as an example of the potential threat that the exploitation of IVEs poses to the United States.

B. CONCLUSIONS

IVEs are a real and pervasive trend in cyberspace that are becoming increasingly important. They are powerful components of modern life that generate real human responses through real human interaction. Their use spans social interaction, business use, marketing, politics, as well as military simulation and training. IVEs are changing the way humans interact and communicate in both social and professional settings. They link users from around the globe in common environments that transcend traditional national boundaries, language, culture, religion, and geography. The DoD cannot afford to ignore this phenomenon.

Information operations are an established and integral part of our military doctrine. The nature of conflict has shifted to a point where non-kinetic effects are preferred over more destructive kinetic alternatives. Winning the hearts and minds of a community and establishing local support can undermine an adversary's control over an area and achieve victory without excessive loss of life. Supporting this shift is the development of new tools and techniques made possible by new technologies and an increasingly globally connected world. The use of IO in IVEs represents such a technique.

China has distinct advantages relating to cyberspace and it is aware of these advantages. It views hacking and cyber warfare as patriotic and nationalistic elements of a comprehensive national defense strategy. China has a large investment in cyber

infrastructure to include its own IVE with active government oversight. China also possesses a population of millions of English-speaking cyber denizens led by a government with a vastly different view of warfare as compared with our own. This combination of elements in an example of a nation that will, if it has not already, exploit IVEs for political and military advantage.

The United States cannot afford to ignore this real and emerging threat. U.S. military operations and dominance in the land, sea, and air domains are dependent on maneuver and dominance in the cyberspace domain. Cyberspace operations must include development of Tactics, Techniques, and Procedures (TTPs) for offensive and defensive employment of IO in IVEs and similar virtual environments. Training should be developed tailored to the roles of officers and enlisted. OPSEC awareness must be stressed.

The DoD must update current operational policies and doctrine across all services that redefine and consolidate understanding of operations and warfare in cyberspace. Specific to IVEs, the DoD must recognize the potential threat that exploitation of IO in IVEs poses, as well as acknowledge the advantages our adversaries have in this arena relative to our own capabilities. Our own organic capabilities must be developed in order to defend against or counter this imminent threat.

The United States must examine the laws of war and modify interpretations or the laws themselves to allow for prosecution of belligerents or allow for the response to hostile acts in cyberspace. The laws of war, as an aspect of public international law, concerning acceptable justifications to engage in war and the limits to acceptable wartime conduct, are virtually obsolete in a cyber war scenario and may become a dangerous constraint to the U.S. in future conflicts.

China (and others) could use our adherence to these laws as a weapon. For example, how should the U.S. respond to unrestricted warfare directed against it by the Chinese? More to the point, what is or is not considered an act of war? A combination of trade warfare in the physical world and a coordinated IO media campaign in

cyberspace and IVEs could have a debilitating effect on the U.S. economy,[27] yet under current law would not qualify as a warlike act. The United States must be prepared to categorize these acts and generate an appropriate response. The United States should not wait until an event occurs to attempt to apply radical new interpretations to international law.

This thesis set out to answer the primary research question of whether it is possible to effectively leverage Information Operations in an Immersive Virtual Environment. This thesis shows that IVEs provide access to large numbers of humans and presented trends that suggest those numbers will grow. It is clear that IO can be leveraged effectively in an IVE. IVEs possess enormous potential for communication and influence. Pursuing continued research into developing this capability reduces the risk that the DoD will realize the potential in this area before falling victim to adversarial exploitation of the same.

C. IMMEDIATE RECOMMENDATIONS

Develop new training curriculum for uniformed service personnel surrounding the risks of IO in IVEs. This should include, but is not limited to, training provided during initial recruit training, formal schools, PME, JPME, and annual operational security training and information assurance/security training. This training should be integrated with existing training and guidance surrounding responsible use of Internet-based capabilities similar to that outlined in MARADMIN 181/10.

Stress the importance of OPSEC awareness and provide tangible indicators that service members can use to assess potential IO activities occurring.

During initial and annual refresher training, convey the risks associated with military members using these environments. Provide simulations[28] that realistically portray the environments where this may occur, as well as realistic demonstrations of methods that adversaries may employ.

---

[27] An example might be a well-timed rumor spread on the Internet, causing artificial and debilitating manipulation of the U.S. stock market.

[28] Simulations should be in the form of an IVE environment in order to provide the relevant context.

Provide a more in-depth study of IO in IVEs to Staff Non-Commissioned Officers and Officers.

Incorporate offensive and defensive considerations for the operational employment of IO capabilities in IVEs into PME curriculum.

Stress operational considerations to senior service members.

D. FUTURE WORK

Conducting research for this thesis naturally presented several new questions and topics. Information Operations and Immersive Virtual Environments are fairly well documented and understood in their respective disciplines; however, operational employment of the latter in the former seems to be a new concept. Those topics and questions are captured in the following pages. The top three priorities are listed first. The remaining topics are presented in no particular order.

1. Concept of Employment

Develop tactical, operational, and strategic employment considerations for the use of IO in IVEs. Conduct research to investigate if tactical or operational employment initiatives will have strategic impacts.

2. Ethical and Legal Challenges

Does high-level military leadership recognize the need not just to develop a defense against adversarial employment of IO in IVEs but also to develop our own offensive and defensive capabilities of IO in IVEs?

How can we convince high level military staff, politicians, and the American public that this is a good or necessary undertaking?

What modifications are required to current laws, acts, and other controls aligned with operating in IVEs (and cyberspace)? Are there capabilities or limitations based on Title 10, Cyber-Law, Patriot Act, Homeland Security, 1st Amendment, international law, and other? Are new laws required?

How do we successfully operate within the constraints of laws and simultaneously allow for effective responses to attacks from adversaries who may not abide by the same?

Do we or other countries currently declare any part of these cyberspace or areas within IVEs sovereign territory? Does activity in/around/at them constitute an act of aggression or war? Example: There are virtual embassies in *Second Life*. Could attack, real or perceived in an IVE (e.g., virtual riot or protest), justify retaliation of some form in the physical world?

3. Measures of Effectiveness (MOE)

Offensive: How will effects be measured? How is success and failure determined? What will metrics be and how will we apply them?

Defensive: How will effects be measured? How do we know if we have successfully defended against IO attacks in IVEs?

4. Control and Oversight

Is this a DoD, NSA, CIA, FBI, DHS, or other capability? What about Joint operations? What are the considerations for coalition or international operations? Will it be a classified or unclassified capability?

5. IO/MMORPG Potential

IVEs and MMORPGs have distinct similarities and usage statistics for MMORPGs suggest that comparable IO capability exists in them. Can IO be effectively employed within MMORPGs?

6. Develop "IO RADAR" for Use in IVEs

The U.S. military knows how to track missiles, submarines, delivery trucks, cell phones, logistics, etc. How do you track IO in IVEs or in cyberspace in general? Are there logical and established heuristics for IO (e.g., A Denial of Service [DOS] attack has an identifiable signature when employed)? Can individual avatars be tracked and followed? Is there a capability that allows for virtual surveillance?

7. Cyber-War and Cyber-Terrorism

Research future work into related and overlapping areas of Cyber War and cyber-terrorism. For example, the use of IO in IVEs to counter or undermine adversarial use of covert communication within IVEs.

8. Further Research with Stanford Labs

The Virtual Human Interaction Lab (VHIL) and Persuasive Technologies Lab, both at Stanford University are both conducting behavioral influence research that has relevance to IO. Consider aligning further research in these areas to understand more of the operational risks and benefits of operations in cyberspace.

9. How Will Presence of IO or Knowledge of its Use Affect Population and Interaction within IVEs?

Conduct research to determine if the conduct of IO in IVEs would cause people to develop alternative collaboration/connection means. Will they continue to use IVEs or will there be a shift in behavior to counter potential IO effects?

Will users simply vacate IVEs negating IO potential and move to another social networking or collaboration tool?

LIST OF REFERENCES

[1] Joint Forces Staff College - National Defense University. Information operations timeline. August 1, 2008. [Online]. Available: http://www.jfsc.ndu.edu/schools_programs/jc2ios/io/io_timeline.asp (accessed May 25, 2010).

[2] Joint Chiefs of Staff. "Information operations." *Joint Publication 3–13*. Washington, DC, February 2006.

[3] J. Scharlat. "Intelligent virtual environment agents (IVEAs): Conducting information operations in virtual environments." M.S. thesis, Naval Postgraduate School, Monterey, CA, 2007.

[4] J. Blascovich, J. Loomis, A. Beall, K. Swinth, C. Hoyt, and J. Bailenson. Immersive Virtual Environment Technology as a Methodological Tool for Social Psychology. *Psychological Inquiry*, vol. 13, pp. 103–124, 2002.

[5] Linden Labs. *What is Second Life*. August 1, 2008. [Online]. Available: http://secondlife.com/whatis/ (accessed May 25, 2010).

[6] Computer Avatar, Wikipedia. (n.d). Available at Wikipedia: http://en.wikipedia.org/wiki/Computer_avatar (accessed May 25, 2010).

[7] *World of Warcraft. World of Warcraft*. September 3, 2008. [Online]. Available: http://www.worldofwarcraft.com/index.xml (accessed May 25, 2010).

[8] *World of Warcraft*. Wikipedia. (n.d). Available at Wikipedia: http://en.wikipedia.org/wiki/World_of_Warcraft (accessed May 25, 2010).

[9] *Second Life*. Land. August 1, 2008. [Online]. Available: http://secondlife.com/land/index.php# (accessed May 25, 2010).

[10] Joint Chiefs of Staff. "Department of Defense Dictionary of Military and Associated Terms." *Joint Publication 1–02*. Washington, DC, April 2001, amended August 2008.

[11] W. Koszarek. "Cyberspace: A Microcosm of Human Activity." CNO SSG XXVI Concept paper. 2007.

[12] U.S. states populations. Wikipedia. (n.d). Available at Wikipedia: http://en.wikipedia.org/wiki/List_of_U.S._states_by_population (accessed May 25, 2010).

[13] Linden Labs. Population data. May 24, 2010. [Online]. Available: http://secondlife.com/statistics/economy-data.php (accessed May 25, 2010).

[14] Linden Labs. Economy blog: User hours. August 1, 2008. [Online]. Available: http://blog.secondlife.com/category/economy/ (accessed August 1, 2008).

[15] Venture Beat. *Second Life* economy growth. April 28, 2010. [Online]. Available: http://games.venturebeat.com/2010/04/28/virtual-worlds-recede-but-second-life-keeps-growing/ (accessed May 25, 2010).

[16] Linden Labs. Linden dollars wiki. August 1, 2008. [Online]. Available: http://wiki.secondlife.com/wiki/Category:Linden_Dollars_%28L$%29 (accessed May 25, 2010).

[17] *Second Life*. Business opportunities. August 1, 2008. [Online]. Available: http://secondlife.com/whatis/businesses.php (accessed May 25, 2010).

[18] Venture Beat. Economic graphs. August 1, 2008. [Online] Available: http://venturebeat.com/2010/01/19/second-lifes-economy-grows-65-to-567m/ (accessed August 1, 2008).

[19] S. Milgram. "The Small World Problem." *Physiology Today* , vol. 2 pp. 60–67, 1967.

[20] P. S. Dodds, R. Muhamad, and D. J. Watts. "An Experimental Study of Search in Global Social Networks." *Science*, pp. 827–829, August 8, 2003.

[21] Linden Labs. Password Security Policy. September 3, 2008. [Online]. Available: http://secondlife.com/policy/security/password.php (accessed May 25, 2010).

[22] J. N. Bailenson, A. C. Beall, J. Blascovich, J. Loomis, and M. Turk. "Transformed Social Interaction: Decoupling Representation from Behavior and Form in Collaborative Virtual Environments." *Presence* (Massachusetts Institute of Technology), vol. 13, no. 4, pp. 428–441, August 2004.

[23] Wireshark. About Wireshark. [Online]. Available: http://www.wireshark.org/about.html/ (accessed May 25, 2010)

[24] B. Nass, and C. Reeves. *The Media Equation: How people Treat Computers, Television, and New Media Like Real People and Places*. Stanford CA: CSLI Publications, 2002.

[25] N. Yee and J. Bailenson. "The Proteus Effect: The Effect of Transformed Self-Representation on Behavior." *Human Communication Research*, no. 33 pp. 271–290, 2007.

[26] B. J. Fogg. *Persuasive Technology: Using Computers to Change What We Think and Do*. San Francisco: Morgan Kaufman Publishing, 2003.

[27] *America's Army*. About. July 2002. [Online]. Available: http://www.americasarmy.com/about/ (accessed May 25, 2010).

[28] S. Mann, A. Vrij, and R. Bull. "Detecting True Lies: Police Officer's Ability to Detect Suspects' Lies." *Journal of Applied Psychology*, vol. 89, no.1, pp. 137–139, February 2004.

[29] L. L. Riggs. "Ohio University Opens Virtual Doors." Campus Technology.com. February 21, 2007. [Online]. Available: http://campustechnology.com/articles/2007/02/ohio-university-opens-virtual-doors_63357376853029654 3.aspx (accessed May 25, 2010).

[30] Youtube. "Ohio University *Second Life* campus." February 15, 2007. [Online]. Available: http://www.youtube.com/watch?v=aFuNFRie8wA (accessed May 25, 2010).

[31] *Second Life*. Education. August 1, 2008. [Online]. Available: http://edudirectory.secondlife.com/ (accessed 25 May 2010).

[32] Zdnet News. Business Meetings in *Second Life*. September 2, 2008. [Online]. Available: http://news.zdnet.com/2422–13568_22–218697.html (accessed May 25, 2010).

[33] Cisco. Telepresence overview. [Online]. Available: http://www.cisco.com/en/US/solutions/ns669/networking_solutions_products_genericcontent0900aecd80546cd0.html (accessed May 25, 2010).

[34] *Second Life*. Business success stories. August 1, 2008. [Online]. Available: http://work.secondlife.com/en-US/successstories/ (accessed May 25, 2010).

[35] Businesses and Organizations in *Second Life*. Wikipedia. (n.d). Available at Wikipedia: http://en.wikipedia.org/wiki/Businesses_and_organizations_in_Second_Life (accessed May 25, 2010).

[36] Youtube. "MyBase." February 16, 2008. [Online]. Available: http://www.youtube.com/watch?v=y68V3BvaFds (accessed September 3, 2008).

[37] FedBizOps. MyBase, 3D on-line training environment software, final statement of need. September 3, 2008. [Online]. Available: https://www.fbo.gov/utils/view?id=d1c8a5dd9b84499fe7114404c4a19705 (accessed May 25, 2010).

[38] FedBizOps. MyBase, 3D on-line training Environment software, request for proposal. September 3, 2008. [Online]. https://www.fbo.gov/index?s=opportunity&mode=form&id=807445bf1dab0abd47b4829a72a8691c&tab=core&_cview=0&cck=1&au=&ck= (accessed May 25, 2010).

[39] DoD. "The national defense strategy of the United States, March 2005." March 2005. [Online]. Available: http://www.globalsecurity.org/military/library/policy/dod/nds-usa_mar2005.htm (accessed May 25, 2010).

[40] Joint Chiefs of Staff. "Doctrine for the Armed Forces of the United States." *Joint Publication 1*. Washington, DC, May 14, 2007.

[41] Q. Liang and W. Xiangsui. *Unrestricted Warfare*. Beijing, China. PLA Literature and Arts Publishing House, 1999. [Online]. Available: http://www.iwar.org.uk/iwar/resources/china/iw/unrestricted-warfare.pdf (accessed May 25, 2010).

[42] G. Jinn. "China's development of asymmetric warfare and the security of Taiwan and the Republic of China." M.S. thesis, Naval Postgraduate School, Monterey, CA, 2004.

[43] *Journal of Information Warfare 7.1*. School of Computer and Information Science, Edith Cowen University, 2008.

[44] D. Cheng. "Unrestricted warfare*:* Review Essay II." *Small Wars & Insurgencies 11.1*, (2000).

[45] J.C. Mulvenon, PhD., "Chinese information operations strategies in a taiwan contingency. Testimony of James C. Mulvenon, Ph.D., Director, Advanced Studies and Analysis, DGI Center for intelligence research and analysis, *before the U.S.-China economic and security review commission hearing 'China's military modernization and the cross-strait balance'*." Sept 15, 2005. [Online]. Available: http://www.carlisle.army.mil/DIME/documents/mulvenon%5B1%5D.pdf (accessed 31 May, 2010).

[46] P. Brookesmith. *Sniper: Training, Techniques, and Weapons*. London: Amber Books, 2000.

[47] T. L. Thomas. *Dragon Bytes. Chinese Information-War Theory and Practice*. Fort Leavenworth, KS: Foreign Military Studies Office, 2004.

[48] S. J. Henderson. *The Dark Visitor*. Chicago, IL: Scott Henderson Publishing, 2007.

[49] G. Peng and Y. Youzhi. *The Science of Military Strategy*, Military Publishing House, Academy of Military Science of the Chinese People's Liberation Army, 2005.

[50] *HiPiHi*. Wikipedia. (n.d). Available at Wikipedia: http://en.wikipedia.org/wiki/Hipihi (accessed May 25, 2010).

[51] Virtual Worlds News. *HiPiHi* interface english translation available. June 9, 2007. [Online]. Available: http://www.virtualworldsnews.com/2007/07/hipihi-interfac.html (accessed May 25, 2010).

[52] *HiPiHi*. What is *HiPiHi*. September 2008. [Online]. Available: http://www.hipihi.com/index_english.html (accessed May 25, 2010).

[53] Information Week. Google tries blocking pornography in China. June 19, 2009. [Online]. Available: http://www.informationweek.com/news/internet/google/showArticle.jhtml?articleID=218100384 (accessed May 27, 2010).

[54] Gigaom. A first-hand look at a Chinese *Second Life*, *HiPiHi*. August 25, 2007. [Online]. Available: http://gigaom.com/2007/08/25/hipihi/ (accessed May 25, 2010).

[55] Virtual Worlds News. Virtual worlds news interview: Hui Xu, *HiPiHi* founder and CEO. August 1, 2007. [Online]. Available: http://www.virtualworldsnews.com/2007/08/virtualworldsne.html (accessed May 25, 2010).

[56] ReadwriteWeb. *HiPiHi* - A virtual world born in China. April 1, 2007. [Online]. Available: http://www.readwriteWeb.com/archives/hipihi_china_virtual_world.php (accessed May 25, 2010).

[57] Wall Street Journal Digital Network. *China cracks down on virtual currencies, for real*. June 29, 2009. [Online]. Available: http://blogs.wsj.com/chinarealtime/2009/06/29/china-cracks-down-on-virtual-currency-for-real/ (accessed May 25, 2010).

[58] *HiPiHi*. Resident levels as of today. June 2009. [Online]. Available: http://service.hipihi.com/community/ (accessed May 25, 2010).

[59] *Second Life* Blogs. Q3 spotlight - user hours by country. April 5, 2010. [Online]. Available: http://blogs.secondlife.com/thread/17094 (accessed June 1, 2020).

[60] R. Rippeon. "Clandestine message passing in immersive virtual environments." M.S. thesis, Naval Postgraduate School, Monterey, CA, 2008.

[61] S. Buculo. “Understanding Cross Cultural Differences During Interaction within Immersive Virtual Environments,” *Proceedings of the 2004 ACM SIGGRAPH international conference on Virtual Reality continuum and its applications in industry*. Singapore: [Online]. Available: http://doi.acm.org/10.1145/1044588.1044634 (accessed May 24, 2010).

[62] CNN Politics. Poll: Support for Afghan war at all-time low. September 15, 2009. [Online]. Available: http://www.cnn.com/2009/POLITICS/09/15/afghan.war.poll/index.html (accessed June 2, 2010).

[63] The New York Times. *Obama is first in their Second Life*. March 31, 2007. [Online]. Available: http://thecaucus.blogs.nytimes.com/2007/03/31/obama-is-first-in-their-second-life/ (accessed May 25, 2010).

[64] *Second Life* Left Unity. Another virtual world is possible - academic study. May 5, 2008. [Online]. Available: http://slleftunity.blogspot.com/2008/05/another-virtual-world-is-possible.html (accessed May 25, 2010).

[65] T. L. Thomas. *Cyber Silhouettes. Shadows over Information Operations*. Fort Leavenworth, KS: Foreign Military Studies Office, 2005.

[66] USJFCOM. FITES demonstration demonstrates emerging technology. March 5, 2010. [Online]. Available: http://www.jfcom.mil/newslink/storyarchive/2010/pa030810a.html (accessed June 2, 2010).

[67] R. O’Harrow Jr. “Spies’ battleground turns virtual.” February 6, 2008. [Online]. Available: http://www.washingtonpost.com/wp-dyn/content/article/2008/02/05/AR2008020503144.html (accessed May 25, 2010).

[68] T. L. Thomas. “China’s Electronic Long-Range Reconnaissance,” *Military Review*, November-December 2008. [Online] Available: http://fmso.leavenworth.army.mil/documents/chinas-electronic.pdf (accessed May 28, 2010).

[69] W. Zhu and T. Chen. *Information War,* 1999.

[70] The Wall Street Journal Digital Network. *Computer spies breach fighter jet project*. April 21, 2009. [Online]. Available: http://online.wsj.com/article/SB124027491029837401.html (accessed May 28, 2010).

[71] The Globe and Mail. “Canadian researchers uncover online spy ring based in China.” April 6, 2010. [Online]. Available: http://www.theglobeandmail.com/news/technology/canadian-researchers-reveal-online-spy-ring-based-in-china/article1524228/ (accessed May 28, 2010).

[72] The New York Times. *2 Chinese schools said to be tied to online attacks*. February 18, 2010. [Online]. Available: http://www.nytimes.com/2010/02/19/technology/19china.html (accessed: May 28, 2010).

[73] DIMACS. *Report to national science foundation of China’s higher education and research in computer science and information technology*. Jan 25, 2007. [Online]. Available: http://dimacs.rutgers.edu/Workshops/China/ChinasHigherEd2_summary.pdf (accessed May 28, 2010).

[74] Time. *Enemies at the firewall*. December 6, 2007. [Online]. Available: http://www.time.com/time/magazine/article/0,9171,1692063,00.html#ixzz0pUWZaAHO (accessed May 28, 2010).

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California